IP-guard 3

User Manual v1.0

Copyright

Note

The information in this document is subject to change without notice and should not be construed as a commitment by TEC Solutions Limited. While every effort has been made to assure the accuracy of the information contained herein, TEC Solutions Limited assumes no responsibility for errors or omissions. TEC Solutions Limited assumes no liability for errors in this document or damages resulting from the use of the information contained in this document.

Table of Contents

Chapter 1 Introduction of IP-guard

1.1 Introduction

Corporate information becomes more important under the era of intellectual economy. The critical factor for success is to protect information effectively. With the fast growth in information technology, internet becomes an important channel to communicate between customers and corporations. Despite its convenience, information is more easily leaked. As important information leakage brings loss to corporations, a comprehensive control of computer usage is important. It controls and reduces the risk of loss caused by leakage of the confidential information and/or abuse of corporate resources and intellectual property.

More and more employees spend their time in browsing websites that are unrelated to work during working hour. Such behavior decreases productivity. Many employees may think that the office computers are their personal property; they can do whatever they want with the computers. Corporations should control and monitor their behaviors in order to enhance productivity and minimize the risk of misuse of computer resources.

According to researches of the Gartner Group and Forrester Research, nearly 50% of time within the MIS department has been spent on computer installation and software upgrading which occupy a large proportion of the computer cost. System administrators spend 70-80% of time working on daily maintenance tasks which increase the cost of computers. Moreover, productivity drops when computer problems cannot be solved immediately. Therefore, it is necessary to reduce the workload of system administrators on minor tasks to increase their productivity so that they can concentrate on computer management tasks and information system enhancement.

IP-guard is powerful software to solve the above problems for corporations. IP-guard can monitor and record the utilization of every computer. Its functions include daily operation statistics, policy management, screen snapshot, real-time recording, asset management, system patch management, software distribution, and remote control, etc. IP-guard can automatically record screen snapshots, record computer utilization, and playback records. With all these functions, corporations can realize the computer resources utilization, secure corporation information, and enhance productivity.

1.2 Major Functions

Corporations nowadays not only protect their physical resources; human resources, intangible assets such as intellectual property, information, and goodwill are also very important. IP-guard provides effective monitoring and managing capabilities to help corporations minimize their risks in information security. IP-guard is an application to effectively monitor and manage corporate network activities, including:

Running Statistics

IP-guard can generate statistics reports on every application process, website browsing, and network flow in order to evaluate the behavior of staffs.

Real-time Monitoring

With IP-guard, administrator can monitor computer usage, including application usage, website browsing history, document operation, printing, screen snapshots, instant messages, and email contents in real time.

Policy Control

Computer restrictions including application usage, website browsing, document operation and printing, network usage, bandwidth, and devices can securely protect corporation information, enhance staff efficiency, and allow corporation to plan resources reasonably.

Real-time Maintenance

System administrators can monitor computers remotely with IP-guard. It controls computers, analyzes, and solves computer problems remotely.

Asset Management

IP-guard records hardware and software asset information in detail. Alert can be sent when there is any change in software or hardware. Asset information can be searched from custom-built query.

Patch and Vulnerability Management

IP-guard frequently checks Windows patches. It automatically downloads, distributes, and installs the patch to agents if new patch is found. Also, it scans for vulnerability frequently with analytical information and repair suggestions.

Software Deployment

IP-guard provides a simple way to distribute documents and deploy third party software to internal computers within the corporation to lighten the workload of administrator and enhance efficiency at the same time.

Characteristics of IP-guard include:

Powerful data compression, archiving and viewing features

Optimized data compress algorithm to ensure high efficiency data access. Historical screen snapshot information is stored in the internal archive system of the server using a specialized compression format. System administrator can backup the archived data to backup storage device. Authorized users can search and view the historical data by selecting the target computer and its recording period.

Data Encryption

Data transfer between workstation and server are encrypted using DES algorithm. With this encryption technology, data is protected from illegal data capture.

System Authentication

Authentication is required for communication between server, agent, and console. Agent workstation can only respond to authenticated server to prevent unauthenticated server connecting to the network to steal data.

Friendly User Interface

Despite powerful monitoring and data management functions, IP-guard has a simple and easy-to-use user interface. All functions are well-organized and visualized in the graphical user interface.

Expandable and Cost-saving Solution

Computer equipment can be fully utilized under IP-guard system. It can be easily deployed from a single workstation to a network environment. Number of managed workstations can also be adjusted. Hence, it reduces the software cost for hardware and network upgrade.

Chapter 2 IP-guard Installation

2.1 Basic Structure

IP-guard system consists of 3 different components: Agent, Server, and Console. It is used on computers inside the network to enhance its security. Agent is installed in every inspected computer. Server is used for database storage and Agent management. Its main duty is to manage the inspected data. Usually, server should be installed on a server class computer with a large amount of system memory and large hard disk capacity. Console is used to audit, control and monitor the computers with Agent installed and examine the log history. In most cases, Console will be installed on the administrator's computer alone, but it can also be installed with Server together on the same computer. The basic structure is shown below:

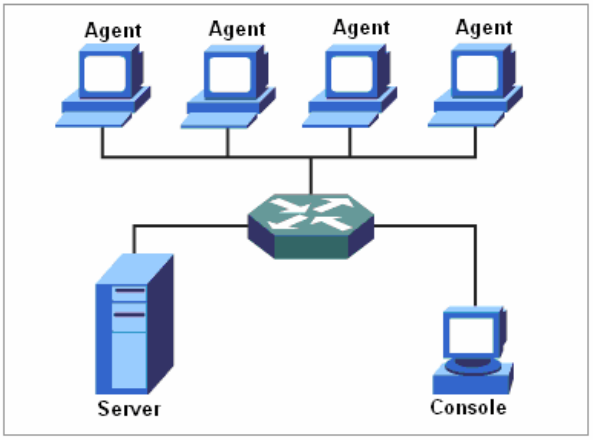


Figure 2.1 Basic System Architecture of IP-guard

Server functions:

- Search the network periodically, manage all the computer with Agent installed and send policy settings and commands to Agents.
- Collect Agent data and save it to the database.
- Backup log history.
- Provide convenient log history management, such as, reading, archiving, and searching.

Console functions:

- Real-time screen capturing on agent computer
- Single or multiple real-time screens monitoring able to display screen snapshots of multiple targets at the same time.
- Set up monitor and control policy
- Play screen history saved in the Server database.
- Search screen history by designated computer on designated date.

Agent functions:

- Collect and save data periodically

- Send the collected data to the Server periodically
- Respond to the real-time screen snapshot capturing request from Console.
- Control the operation of the user and computer according to the system policy.

2.2 Software Requirements

Module	System Requirement	
Database	SQL Server 2000 SP4 or above / SQL Server 2005 SP1 or above MSDE SP4 / SQL Server 2005 Express	
Server	OS	Win2000 SP4/XP SP2/2003 SP1/Vista
	Minimum	Pentium III 500/256MB 10GB Hard disk space
	Recommended	Pentium 4 2G/512MB 50GB Hard disk space
Console	OS	Win2000 SP4/XP/2003/Vista
	Minimum	Pentium 166/64MB 10MB Hard disk space
	Recommended	Pentium III 1G/256MB 100MB Hard disk space
Agent	OS	Win Me/NT4/2000/XP/2003/Vista
	Minimum	Pentium 166/64MB 10MB Hard disk space
	Recommended	Pentium III 500/128MB Hard disk space

Table 2.1 Software Requirements

[Important]

Server & SQL Requirements
■ If the Server is installed on Windows 2000 SP4, please make sure the system is updated with service patch: **Win2000-KB891861-v2x86-*.exe**
■ If you are using Microsoft Server 2000, please make sure that it is updated with Service Pack 4: **SQL2000-KB884525-SP4x86-ENU.exe**

2.3 Installation

2.3.1 Database Installation

Prior to IP-guard installation, database must be installed on the IP-guard server. IP-guard supports SQL Server 2000 SP4 or later, SQL Server 2005 SP1 or later for database. If licensed SQL Server is not available, please install the free MSDE SP4 or SQL Express 2005 provided by Microsoft. Below are the instructions for installing MSDE:

[Important]

SQL Server Limitations
■ The limitation of Database size on free MSDE and SQL Express 2005 are 2G and 4G respectively. With this limitation, it would affect the stabilities of server. We strongly recommend using Enterprise

version if there are many agents and too much data has to be stored in the database.

- Please ensure that SQL Server 2000 is installed together with SP4, and SQL Server 2005 is installed together with SP1. If IP-guard server cannot startup properly, please go to **Windows Control Panel → Administrative Tools → Event Viewer → Application Log** to confirm the version of SQL Server

MSDE Installation

[How to]

1. Double click the MSDE setup file, and then it will display a default path for file extraction, please select a path and extract the setup files.

2. Open the directory where the setup files extracted, under the MSDE folder, there is a file named setup.ini.
   Default content of setup.ini:
   [Options]
   Please edit the file by adding the follow line:
   [Options]
   BLANKSAPWD=1
   Save the setup.ini after editing.

3. Run the setup.exe under the MSDE folder to start the installation.

4. Run the SQL Server Network Utility. Open a command prompt and type: **c:\ svrnet.exe**
   Make sure that **Name Pipes** protocol is enabled.

SQL Server 2005 Express Installation

We recommend installing **Express Edition with Advanced Service** version

[Prerequisite]

1. **IIS 5.0 or above**
   If your Windows does not install with IIS, please go to **Windows Control Panel → Add or Remove Programs → Add or Remove Windows Components** to install IIS
2. **.NET Framework 2.0**
   Please go to Microsoft website to download .NET Framework 2.0 (x86) and install
3. **Windows Installer 3.1**
   Please go to Microsoft website to download Windows Installer 3.1 and install

[How to]

1. Download SQL Server 2005 Express Edition with Advanced SP1 from Microsoft. Double click the **SQLEXPR_ADV.EXE** to start the setup. After reading and accepting the **End User License Agreement**, click **Next** to continue
2. Prior to installing SQL Server, there is some software components required to install. Click **Next** to continue SQL Server setup when all required components are installed.

3. All necessary conditions are listed, click **Next** to continue
4. In the **Registration Information** windows, unclick the option **Hide advanced configuration options**. Click **Next** to continue
5. In the **Feature Selection** windows, make sure **Management Studio Express** is selected. Click **Next** to continue
6. In the **Instance Name** windows, make sure **Default Instance** is selected. If another option is selected, it will cause the IP-guard server cannot start up properly.
7. In the **Service Account** windows, select **Use the built-in System account** and then select **Local system**. Click **Next** to continue.
8. The remaining parts should be followed by the default settings until the installation completed.
9. Open the **SQL Server Configuration Manager** from **Start → All Programs → Microsoft SQL Server 2005 → Configuration Tools → SQL Server Configuration Manager**
10. In the left panel, expend the **SQL Server 2005 Network Configuration** and then click the Protocols for **MSSQLSERVER**, double click **Named Pipes** to make the status **Enabled**

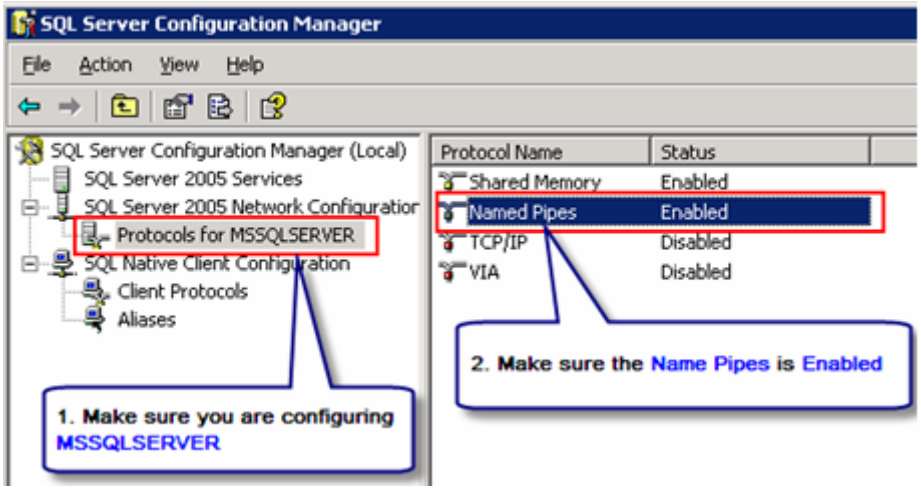


Figure 2.2 SQL Server Configuration

11. Expend the **SQL Native Client Configuration** and then click the **Client Protocols**, double click **Named Pipes** to make the status **Enabled**.

2.3.2 Server and Console Installation

Make sure the SQL Server or MSDE is started up

[How to]

1) Double click IPguard3.exe, select the installation language, and then click **Next**;

2) Main installation interface will show up, click **Next**;

3) The installation process prompts the default installation path. Users can select another path for installation. Please select a partition with a larger storage size for IP-guard server installation;

4) The installation process prompts the types and components. Users can select IP-guard server and console as they need. Click **Next**;

5) Select the path of short-cut inside the “Start menu”. Click **Next**;

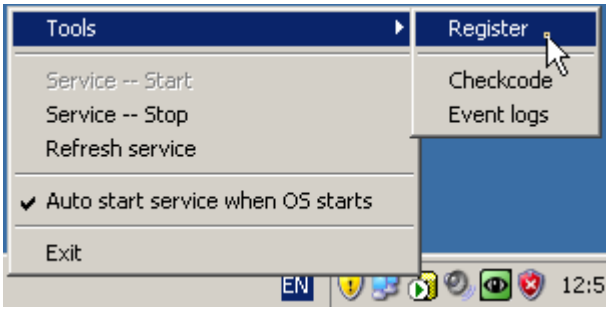
6) After verifying the settings, click **Install** and wait for the installation process to complete. Then, click **Finish** to end the installation. The server will startup and the **IP-guard Service Manager** will be displayed on the task bar.

[Important]

Event Viewer helps trace the installation problems
During the server installation, installation process will determine the operation system and the version of the SQL Server. If the installation is not successful, please check the error message in **Windows Event Viewer → Application** to analyze the problems

2.3.3 Server Registration

IP-guard will generate a trial key for 30-days trial at the first time installation, the serial number is composed of 6 groups of 4 digits string.



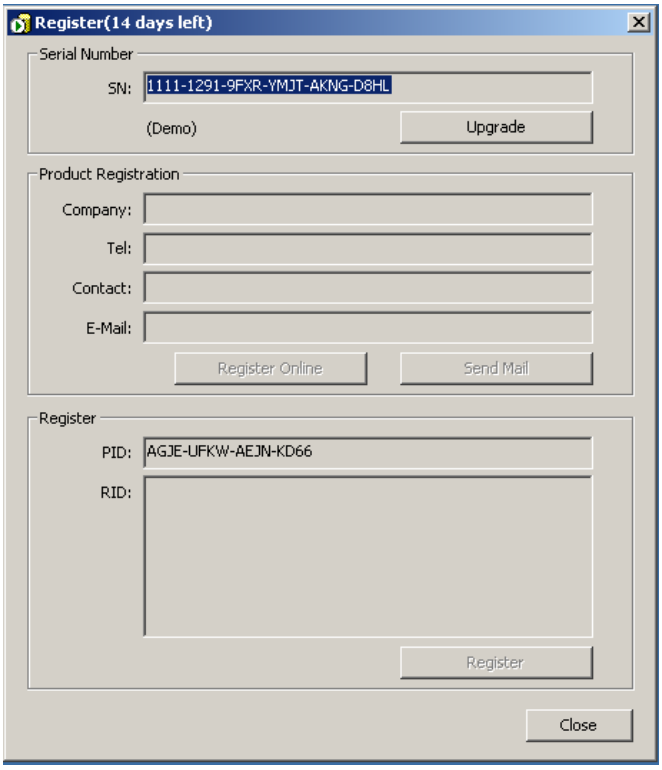


Figure 2.3 Server Registration

[How to]

1. Right click **IP-guard Service Manager→Tools→Register**, then input administrator password to enter the registration interface

2. Click the **Upgrade** button, the serial number text field becomes **editable**, input the licensed serial number

3. Click **Confirm** button to confirm the input serial number. If the input is correct, system will pop up a confirmation dialogue and remind you to activate the system. You have to register the product to obtain the register ID. Only with valid register ID input, the whole registration procedure is so-called completed.

There are two methods to complete the registration:

1. Online Please fill in the product registration information with Company Name, Contact Person, Contact Number and email address. Click **Register Online** button, then the Register ID will be returned and displayed in the Register ID [RID] field.
A dialogue box with system message " " showed will pop up to confirm the registration.
Click Close button to leave the registration interface.

2. Email Please fill in the product registration information with Company Name, Contact Person, Contact Number and email address. Click **Send Email** button.
Email will be sent to your registered email address with Register ID, please copy and paste the Register ID into Register ID [RID] field, then click **Register** button to confirm the registration.
A dialogue box with system message " " showed will pop up to confirm the registration.

Click Close button to leave the registration interface.

Table 2.2 Registration Methods

[Important]

About Registration...
■ You have to activate the product with input valid register ID within **15 days**. Otherwise, the system will be stopped automatically and cannot work properly.
■ If your server cannot connect to Internet or other reasons, please email us with your Serial Number [SN] and Product ID [PID], we will help you process the registration individually.

2.3.4 Checkcode Setting

Checkcode is a unique identifier between server and agent. The checkcode stored in agent must be matched with server's checkcode, then the server is granted to manage the agent. In case of more than one server running at the same time in a network, this avoid the agent is managed by another server which may not belong to its original parent server. So, we highly recommend the system administrator first set the checkcode before deploying any agents.

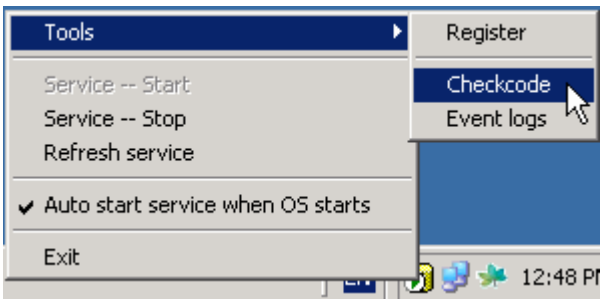


Figure 2.4 Set Checkcode

[How to]

After the server starts up at the first time, right click the **Service Manager** icon and select from the popup menu **Tools→Checkcode**. System would request to input administrator login and password before setting the Checkcode. To confirm the setting, please input the Checkcode twice. Click **OK** button to complete the setting.

The default Checkcode is empty. Once the checkcode is new set, reset or updated, this data will be updated to connected agents automatically.

[Important]

About Checkcode...
■ System Administrator has to memorize or record this Checkcode in the save place. In case the operating system is required to be re-installed or IP-guard is required to install on a new server, the last Checkcode must be input after the re-installation completed. Otherwise, those existing agents could not be connected to the new setup server because their checkcode are not matched. In this case, all agents must be re-installed.
■ If agents not appear in the Console, please go to IP-guard **Console → Events Log → System** to check whether it is checkcode error or not

2.3.5 Server Log

To examine the IP-guard server activity in details, please go to **Windows Event Log**. System Administrator may use the information to analyze the server problems.

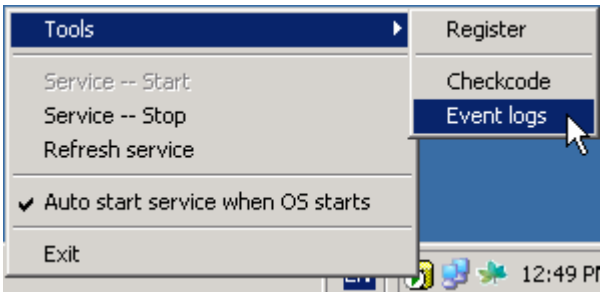


Figure 2.5 View Event Logs

[How to]

Right click the **Service Manager** popup menu **Tools → Event Log**. Click the **Application** from the left-hand-side panel of the **Event Viewer** to check the OSERVER3 process logs including the startup, stop or error status of oserver3.exe.

2.4 Agent Deployment

There are three installation methods to install agents: Direct, Remote and Logon Script Installation methods. Depends on the deployment environment, system administrator can choose either one for the agent deployment

2.4.1 Direct Installation

To generate executable agent program, on IP-guard server, **Start → All Programs → IP-guard V3 → Agent Install Generator**, showed as following:

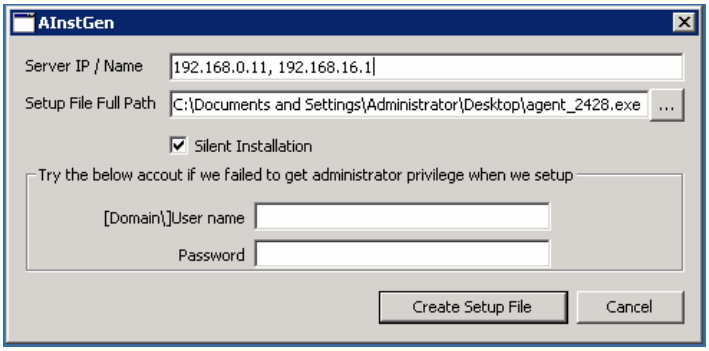


Figure 2.6 Agent Generator

Input the following fields, finally click **Create Setup File** button to generate the agent program

Server IP Address	- Default is the IP of the local machine. If more than one IP addresses, you can input using comma "," to separate the IPs e.g. 192.168.1.223, 58.177.209.222 - Static IP or Dynamic DNS is allowed to input
Setup File Full Path	Input or Select the path and filename of the Agent setup file to be created
Silent Mode [optional]	- if selected, no user interface will show up during installation
Login & Password [optional]	- if the logon windows account is not administrator, the created agent program may not setup successfully. If so, you should input the administrator's login and password before the program packed.

Table 2.3 Settings of Agent Generator

2.4.2 Remote Installation

[How to]

Using Remote Installation tool can help you install agents remotely and massively at a time. On the IP-guard server, click **Start → All Programs → IP-guard V3 → Agent Remote Installer** to start the installation.

[Functionality]

1. Scanning Settings

By default, the system only scans all computers from IP-guard server's network segment. If you want to extend the searching area, go to **File → Scanning Settings**. In the opened dialogue, you can add the IP range.

2. Color Representation of the computer icons

Icon	Color	Window NT4.0/2000/XP	Window 95/98/ me	Online or not	Agent Installed or not
	Deep blue	Yes	No	Yes	No
	Deep blue	No	Yes	Yes	No
	Gray	Yes	No	No	No
	Gray	No	Yes	No	No
	Light Blue	Yes	No	Yes	Yes
	Light Blue	No	Yes	Yes	Yes

Table 2.4 Color Representation of the computer icons

3. Installation

Click which computers you would like to install the agent. After selected, go to **Operation → Install** to start the installation. During installation, the administrator login and password are required if the current logon session is not administrator. The near bottom panel showing the details of installation status, if any failures happened, the panel will show you the description and corresponding error code.

[FAQ]

If failure occurred during remote installation, please check the following items are available in your targeted computer:

1) If the current logon session does not grant administrator right, at this time the system would pop up a dialogue box to request input the login account and password with administrator rights.

2) Check **ADMIN$** share is opened or not. Go to DOS Command Promote and type: **net share** command to see whether **ADMIN$** is already opened or not. If not, then type **net share ADMIN$** to invoke this function

3) Check any shared folders function is available. If not, please try to share a folder to invoke this function. For example, right click a folder, select **Properties → Sharing**. Then Select **Share this folder**. Input Share name and define permission. Click **OK** to invoke the shared folder function

[Important]

About Agent Installation...

- This installation method only works on Windows NT4.0/2000/XP. If you need to install agents on Windows 9x/ME, you have to use Direct Installation method.
- Because of some local security policies settings in Windows NT may affect the normal operations, remote installation method does not 100% guarantee. If you have followed the above checking and fulfilled the requirements, but still failed, we would recommend using **Direct Installation** method (please refer to Section 2.4.1).

2.4.3 Logon Script Installation

If your local area network has a domain server，you can use this method to deploy IP-guard Agent to computers in your local area network. Use the Logon Script Manager to edit logon scripts of selected users in domain server. When those users use their computers to log on to the domain server, the logon script is run and IP-guard Agent will be installed to the selected computers remotely.

[How to]

1) Download the program first:
   http://www.ip-guard.com/Down/V3/supp/IP-guard3_LogonScript_20071129.zip
2) Extract the zip file, then copy and paste the LogonScript folder to Domain Server any locations e.g. place it in Desktop or C:\
3) On the IP-guard Server, using **Agent Installation Generator** to generate the agent setup program, name **ASetup.exe** (Please refer the details in Section 2.4.1 Direct Installation how to generate the setup program)
4) Copy and paste the **ASetup.exe** into LogonScript folder
5) Execute the **LgnManV3.exe**
6) The interface of Logon Script Manager is shown as following, **LgnManV3.exe** will automatically scan and show all existing domain users. The user icon for the green color means that logon script has included our Agent installation settings.
7) Select required users to set installation script, you can use **CTRL** or **SHIFT** keyboard to select multiple users and right-click to select the users.
8) Click the button **Set Script** after you have selected required users.
9) When the selected users log on to the domain, the logon script will be run and IP-guard Agent will be installed to computers of the selected users.
10) Once IP-guard Agent is installed to the selected computer, you can restore the logon script of the selected user to the original logon script.

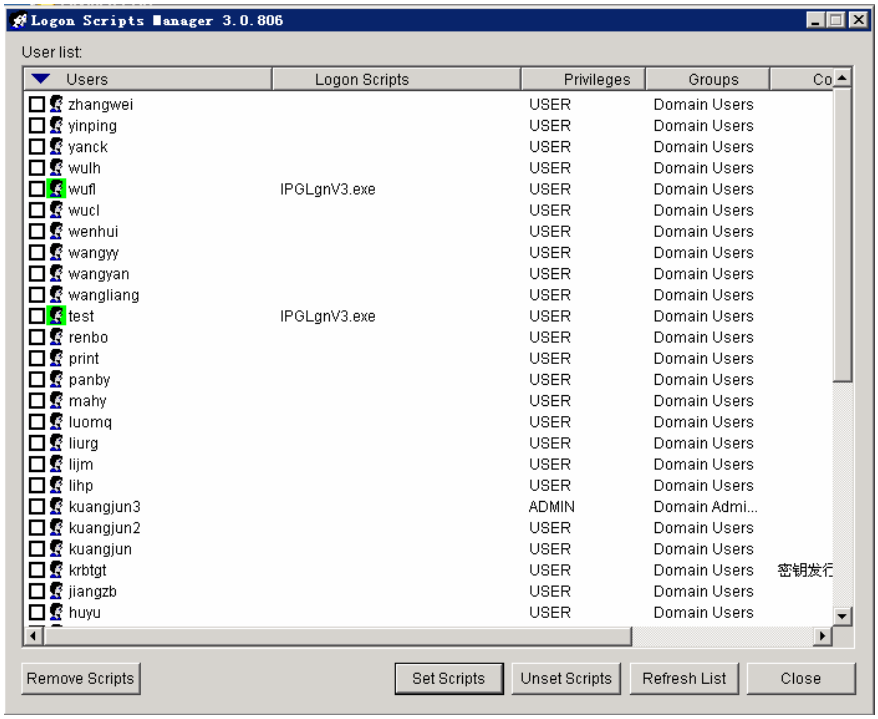


Figure 2.7 Logon Script Manager

[Functionality]

Set Scripts	Add our installation command in logon scripts of selected users.
Unset Scripts	Delete our installation command in logon scripts of selected users.
Refresh List	Rescan user list
Remove Scripts	Set selected users as having no logon script (It will not delete logon script)
Close	Exit the program.

Table 2.5 Logon Script Manager Functional Buttons

[Important]

About Logon Script
When we set selected users as having no logon script, our program will not delete script files .You have to clear the files yourself, and please make sure the files are not used by any script file before you delete them.

2.5 System Upgrade

2.5.1 Server and Console Upgrade

It is easy to upgrade server and console using our Upgrade pack.

[How to]

1. Go to **Windows Control Panel → Administrative Tools → Service** to stop the following 2 services: **OCULAR V3 SERVER** and **OCULAR V3 UPDATE**
2. Go to **task manager → Process**, stop the **service manager OControl3.exe** and **console OConsole3.exe**
3. Now you can start the upgrade process by executing the upgrade program. In the upgrade program, you can see your current version and upgrade version details. Click **Upgrade** button to start. OR you can upgrade using IP-guard full package to replace the existing one completely.
4. After completed, go to **Windows Control Panel → Administrative Tools → Service** to start the **OCULAR V3 SERVER** and **OCULAR V3 UPDATE** manually. (If you are using IP-guard full package method, the server will start up automatically)

2.5.2 Agent Upgrade

Once the server is upgraded successfully, the corresponding agents will be upgraded automatically. The agent machine must be restarted to complete the system upgrade.

2.6 Uninstall IP-guard

2.6.1 Uninstall IP-guard Server and Console

[How to]

1. Close all running Console
2. Go to **All Programs → IP-guard V3 → Uninstall IP-guard V3** to uninstall IP-guard or go to **Control Panel → Add/Remove Program** to uninstall IP-guard

 **[Important]**

Uninstall agents first before...
If you want to remove all IP-guard agents, Console and Server, please delete all agents first using Console before removing IP-guard. Otherwise, the agents are still running in every computer installed with IP-guard agent even the IP-guard Server is removed

2.6.2 Uninstall IP-guard Agent

To uninstall IP-guard agents, you can either do it from IP-guard Console or agent side machine. Once the agent is uninstalled, that agent will not be guarded by IP-guard anymore unless the agent is re-installed.

From IP-guard Console

[How to]

1. Select the agent from **The Whole Network** tree that you want to uninstall. If you want to uninstall all agents at a time, please click **The Whole Network**.

2. After selected, there are 3 ways to uninstall the agent:

2a) From the toolbar, select **Control → Uninstall Agent** or

2b) Right click the agent from **The Whole Network**, select **Control → Uninstall Agent** from the menu or

2c) Go to **Tools → Computers**, click the **Uninstall** or **Delete** button

Notices that the difference between the function of **Uninstall** and **Delete** button

- **Uninstall** button: the agent is uninstalled without releasing agent license
- **Delete** button: the agent is uninstalled as well as releasing agent license

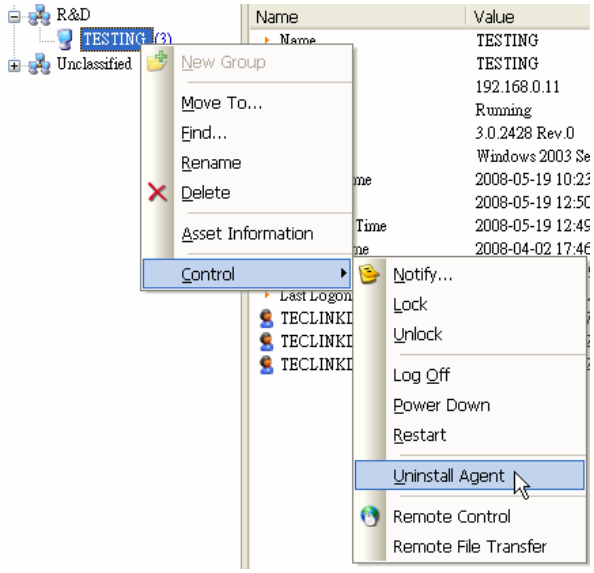


Figure 2.8 Uninstall Agent

From Agent side

For some agents that cannot connect to IP-guard server (i.e. the agent in offline mode), we provide another way to uninstall, the steps are as following:

[How to]

1) Go to **Start → Run**, type **agt3tool ocularadv** command

2) Select **Uninstall Agent** and then click **Generate** button

3) Inform your System Administrator about the **Operate Code** showed in the **Check confirm code** dialog box

4) When a System Administrator gets the Operate Code, go to **IP-guard Console → Tools → Agent Tool → Confirm-Code Generator**, input the **Operate Code** in the field of **Agent Operate Code**. Then click the **Parse** button, the agent information will be showed in the bottom textbox

5) Click the **Generate** button, the **Confirm Code** in Blue color will show in the **Confirm Code Information** box. The System Administrator should tell the **Confirm Code** to the agent user.

6) Once the agent user gets the **Confirm Code**, input it in the field of Confirm Code to process the un-installation immediately

[Important]

About Agent Un-installation...

- Notices that only uninstall agent not exactly delete the agent as the agent license has not been released indeed according to the above methods **2a** and **2b**. If you only uninstall the agent, you will find that the agent still appearing in the **IP-guard Console** (i.e. **The Whole Network** tree) and its icon displayed in dark gray color. To delete the agent completely after uninstalled:
  1. Go to **IP-guard Console → Tools → Computers**, select the agent from the list that you want to delete completely
  2. Click **Delete** button. This action implied that the agent completely deleted and removed from IP-guard. Notices that if you only click the **Uninstall** button, this action implied that the agent will only be uninstalled **without** releasing the agent license.

  To check the agent is deleted completely or not:
  - The agent will not appear in **The Whole Network Tree**
  - Go to **IP-guard Console → Tools → Computers**, the agent should not be listed and the total number of licenses should be decreased

Chapter 3 IP-guard Startup

3.1 IP-guard Console

3.1.1 Logon Console

Before starting the console, IP-guard server must be running.

[How-to]

1. Go to IP-guard default folder and click **OConsole3.exe OR** Go to **Start → All Programs → IP-guard V3 → IP-guard V3 Console**. The Logon windows popped up (see Figure 3.1)

Figure 3.1 IP-guard Login Windows

Server	Input IP address, Computer Name or Dynamic Domain Name
Account	- By default, the account for administrator is **admin** and the account for auditor is **audit** - After logon to the Console, the administrator can create different accounts with different access rights (**IP-guard Console→Tools→Accounts**)
Password	- By default, the password for admin is empty - After logon to the Console, the administrator can edit the password from **Tools → Change Password**.

2. Input correct account and password, click **OK** to logon to Console

When IP-guard connection is disconnected, or you need to logon to another IP-guard server or you need to use another role to logon IP-guard, please go to **Tools→Relogin** to logout current session and re-login based on your need.

[Important]

About Service Manager status...

Make sure the server is running properly: the color of the **Service Manager** should be like this:

- If the status of the Service Manager is , it indicates that IP-guard server is still in initial stage, not completely running. In this case, please wait until the color of the icon changed to .
- If the status of the Service Manager is , it indicates that IP-guard server is stop. In this case, right click **Service Manager → Service – Star**t to start IP-guard server

3.1.2 Change Password

You can change password to prevent others using your account to login to the system and perform illegal operations.

Logon to the Console, select **Tools → Change Password** (see Figure 3.2). In Change Password dialogue box, input the old password (the password is blank for the first time). Then, enter New Password. In Confirm field, re-enter the same new password to make sure the new password is entered correctly. User can only change password of the current login account. The new password will be activated after it is saved in the server module.

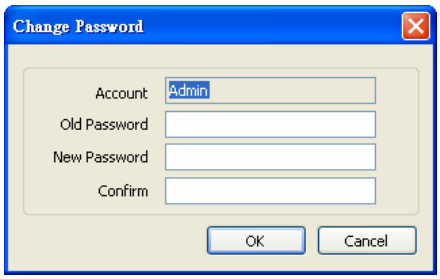


Figure 3.2 Change Password Windows

3.2 Using IP-guard Console

After login to the console, user will see the following user interface (see Figure 3.3). The user interface consists of menu, tool bar, status bar, and main area. The left side of the main area is the console tree of computer (group) and user (group) on the network. The right side of the main area is the data view.

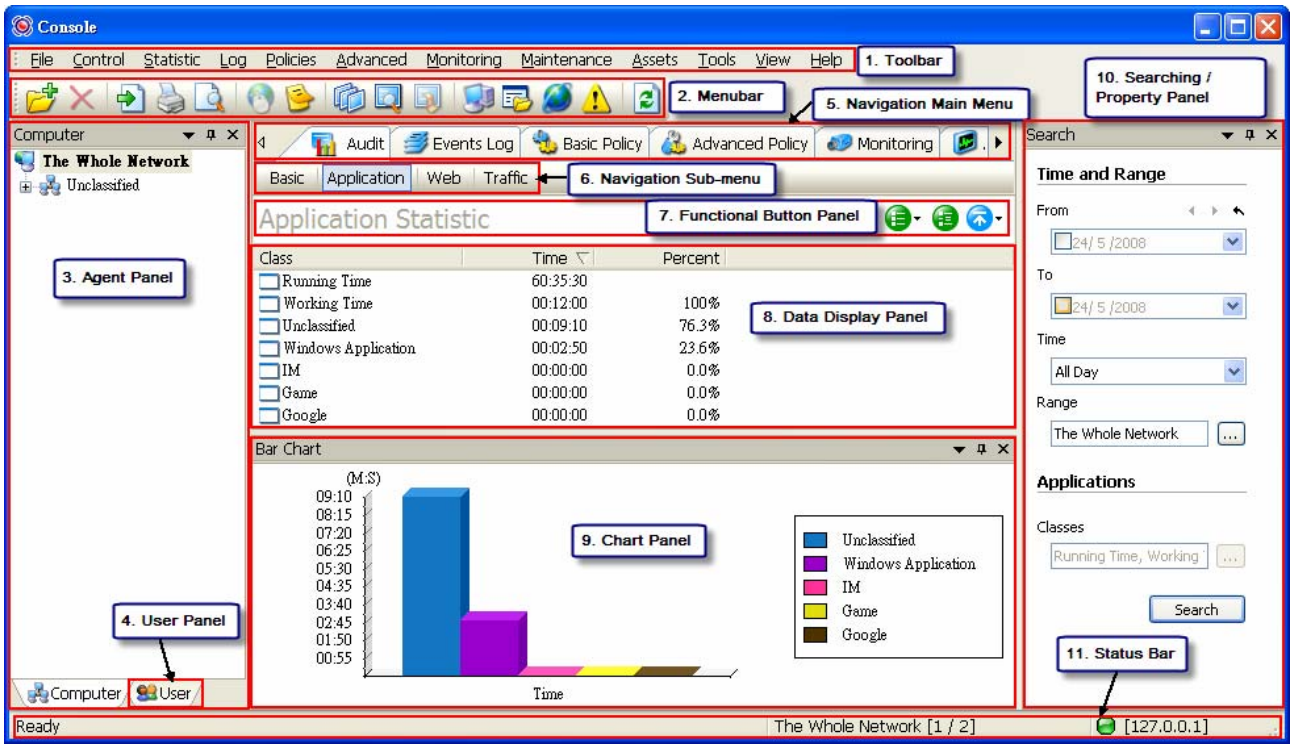


Figure 3.3 IP-guard Console

[Functionality]

IP-guard Console Panel

1. Toolbar	Includes all system menu
2. Menu bar	includes the common functions
3. Agent Panel	In the left window to display all installed agents list under **The Whole Network** tree and the corresponding computer grouping
4. User Panel	In the left window to display all agents' logon account user list under **The Whole Network** and the corresponding user grouping
5. Navigation Main Menu	Quick access to the main functions: Audit, Events Log, Basic Policy, Advanced Policy, Monitoring, Maintenance
6. Navigation Sub-menu	Quick access to the specific functions belonging its grouping
7. Functional Button Panel	Provide different functional buttons e.g. for data sorting, add/delete/apply policy etc.
8. Data Display Panel	Core view – all data display here
9. Chart Panel	For audit functions with statistical data, the corresponding chart displays here
10 Searching Panel / Property Panel	- Searching Panel: For searching purpose in audit, events log, IM and email monitoring - Property Panel: For policy settings purpose
11. Status Bar	Display current system status

Table 3.1 IP-guard Console Interface

Color Representations of Agent Icons:

Icon	Color	Definitions
	Light Blue	Agent is running
	Light Grey	The computer agent module is not running. The computer may be turned off or not connected to the network
	Deep Grey	The agent is un-installed

Table 3.2 Color Representations of Agent Icons

Color Representations of User Icons:

Icon	Color	Definitions
	Light Blue	The agent user is running
	Light Grey	The agent user is not running. The user may not logon to the agent computer

Table 3.3 Color Representations of User Icons

Common Search Conditions

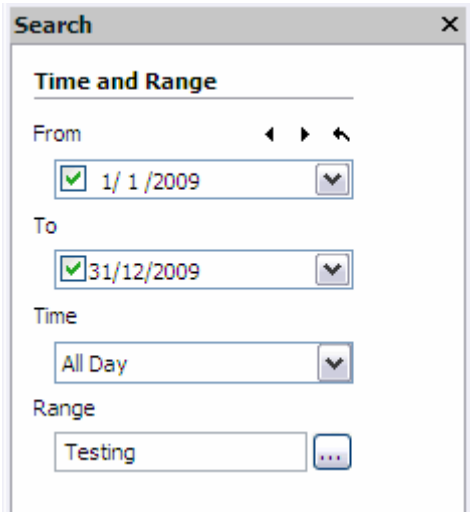


Figure 3.4 Common Search Panel

Date Range For the designated date range, the default start time and end time are not clicked, that is, all log data are searched and display as results. To specify the date range, click the start time and end time:

Icon	Descriptions
◂	Select the date as the start time from the calendar
▸	Select the date as the end time from the calendar
↰	Restore to default setting

Time IP-guard has several defined time types (All Day, Working Time, Rest and Weekend) which can be found in **Tools → Classes Management → Time Types** (see Figure 3.5). System Administrator can also define new time types for their preferences to facilitate the queries.

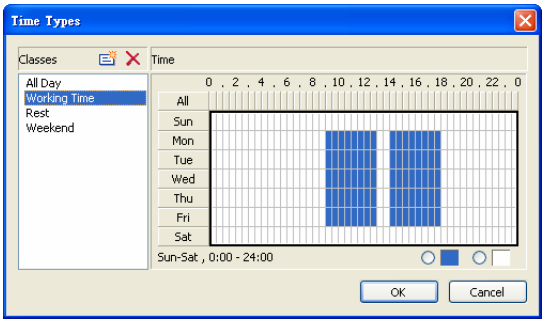


Figure 3.5 Classes Management – Time Types

Network Range Click the … button to select the network range, either a single computer, group or the entire network for query

Table 3.4 Descriptions for Common Search Conditions Functions

Common Log

In the event log, including every common log, email log, instant messenger log, it commonly includes the following contents:

Time	The time for the detailed log
Computer	The log records belonging to the client machine, the computer name here is recorded by IP-guard showed in the agent panel
User	The log records belonging to the user, the user here is recorded by IP-guard showed in the user panel

Table 3.5 Descriptions for Common Log Records

3.3 Computer and User Operations

3.3.1 Basic Information

Select from menu **Statistic→Basic Information** to view the basic information of the computer, computer group, user, and user group (see Figure 3.6). The console displays the running status of the computer and agent when selected a computer.

1) Computer Basic Information

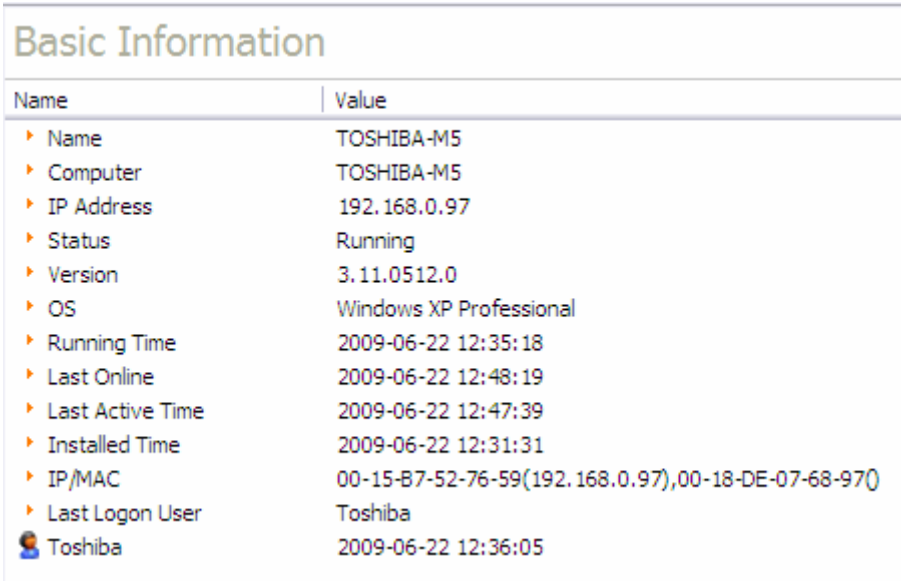


Figure 3.6 Computer Basic Information

Name	The name displayed in the Computer Tree, in order to facilitate management, the name can be changed. If not changed, the name is same as computer name
Computer	It is a real Windows computer name
IP Address	Computer's IP address
Status	Agent status: Running, Offline, Uninstalled
Version	IP-guard agent version
OS	Agent's OS version

Running Time	Agent's startup time. This time only displayed if the status is running. Otherwise, it will not be displayed
Last Online	The last communication time between IP-guard agent and server
Last Active Time	The last active time means the recorded time of the last activities of the agent done in Windows
Installed Time	The first installed time of agent
IP/MAC	The agent's IP/MAC address
Last Logon User	The last logon user in that agent computer. The status of idle or lock also displayed here

Table 3.6 Computer Basic Information Fields Descriptions

Windows server allows more than one concurrent connections connected, in this case, the Basic Information also displays all current connections' logon user information and the logon time (see Figure 3.7)

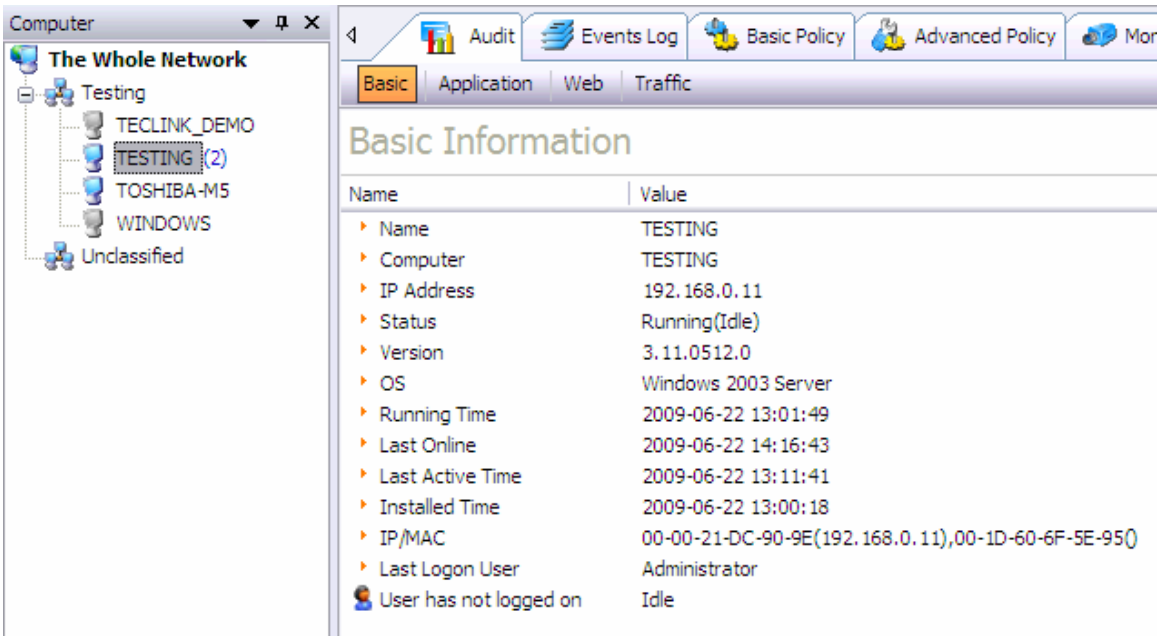


Figure 3.7 Computer Basic Information – Concurrent Logon Information

2) Computer Group Basic Information

Select a computer group will display all computer status under the selected group including computer name, IP address, operating system, and number of user login to the computer (see Figure 3.8).

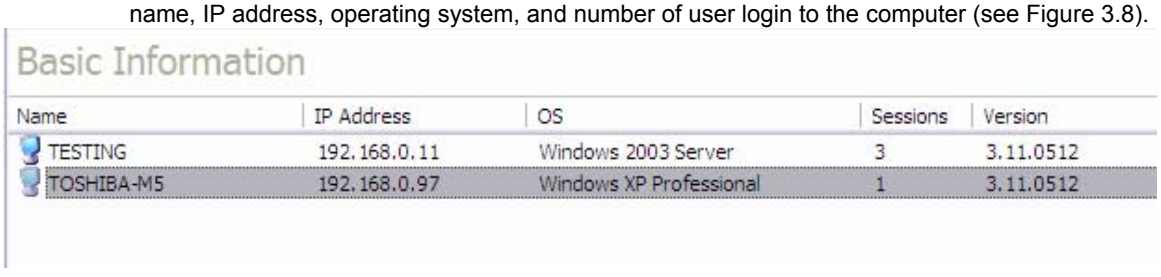


Figure 3.8 Computer Basic Information – Computer Group

If **The Whole Network** selected, IP-guard Console displays all computer groups. Click the button can view all computers belonged to that group (see Figure 3.9)

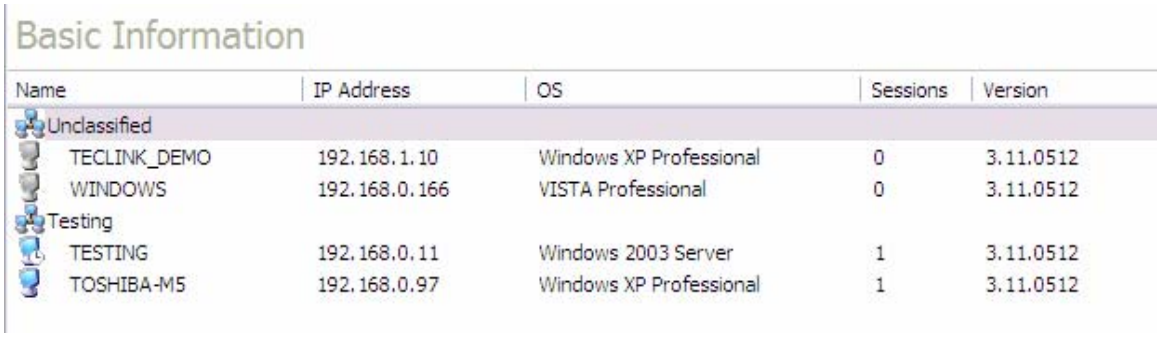


Figure 3.9 Computer Basic Information – Expended Information

3) User Basic Information

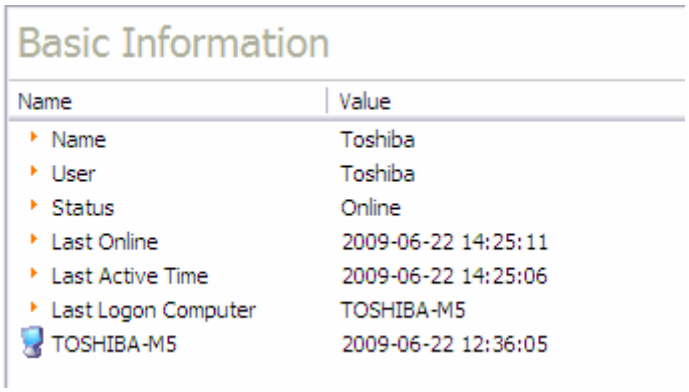


Figure 3.10 User Basic Information

Name	The name displayed in the User Tree, in order to facilitate management, the name can be changed. If not changed, the name is same as user name
User	It is a real Windows logon user name. If it is a local user, it displays the logon name; if it is a domain user, it displays as domain\username
Status	Agent status: Online, Offline etc.
Last Online	The last communication time between IP-guard agent and server
Last Active Time	The last active time means the recorded time of the last activities of the logon user done in Windows

Table 3.7 User Basic Information Fields Descriptions

If the user logons to different computers using the same account, all information about the logon computers and logon time will also display below the Last Logon Computer (see Figure 3.11)

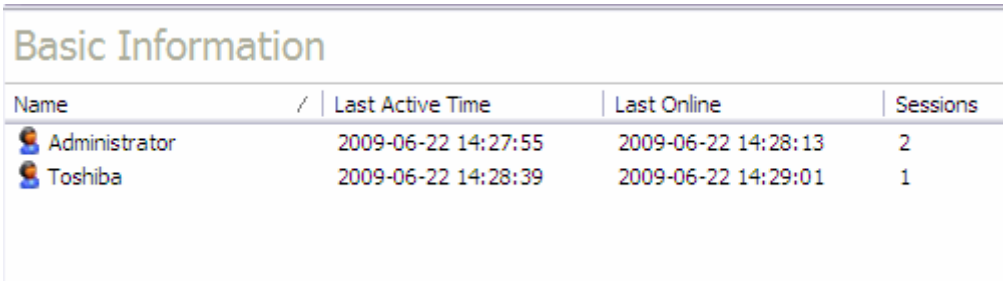


Figure 3.11 Same user account logons to different computers

4) User Group Basic Information

Select a user group will display all user status under the selected group including user name, last online time, last active time, and number of computers login (see Figure 3.12)

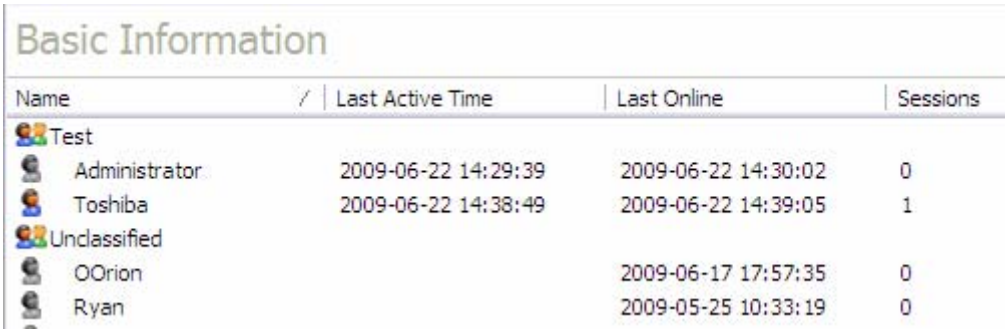


Figure 3.12 User Basic Information – User Group

If **The Whole Network** selected, IP-guard Console displays all user groups. Click the button can view all users belonged to that group (see Figure 3.13)

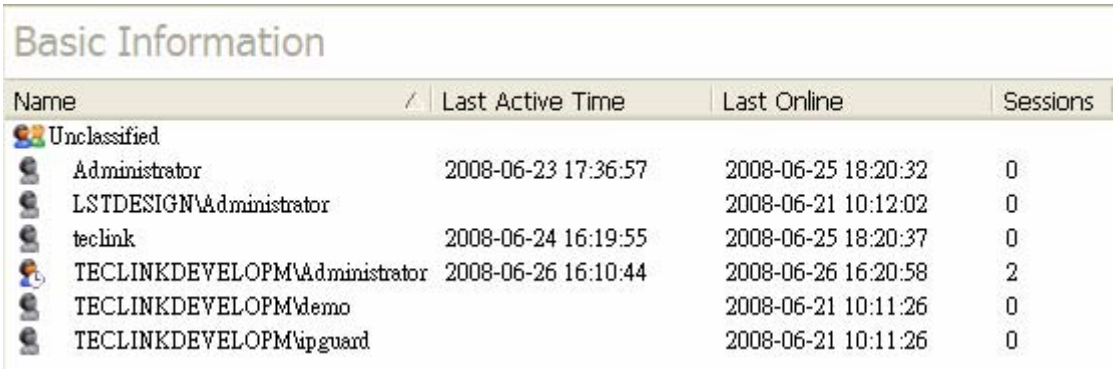


Figure 3.13 User Basic Information – Expended Information

3.3.2 Grouping

By default, all new installed agent will be grouped into **Unclassified** group. To facilitate the computer/user management, System administrator can create some groups and classify them into target groups.

New Groups

Computers and users are displayed in the console tree. Groups can be set according to the actual situation. Then, assign users and computers into different groups. From computer groups and user groups of the

console, computers and users under the group can be managed.

Select the whole network or any group, select **File→New Group** will add a new group in the console tree and allow administrators to name the new group. Administrator can define multi-level groups for the organization. The operation of user group is identical.

Assign to group or changing groups

To assign a computer or user to a group, we can select the computer or user, select **File→Move to** and choose the target group. Then the computer and user will be moved to the selected group.

Alternatively, we can also use mouse drag. Select the target computer or group and drag it to a group. Then the selected computer will be moved to the destination group.

☞ **Hints:**

The default group, **Unclassified**, for computers and users. **Unclassified** group cannot be deleted, renamed, or add new sub-group within.

3.3.3 Find

Administrator can specify a computer or user quickly through the **Find** function to search related log data

Search Computer

In the Computer Tree Column, select **File→Find**. Input the search conditions e.g. computer name or IP address.

The matched results display in the listed box, double click any one record will be directed to related log or policy settings

Search User

Switch to the user column, select File→Find. Input the search conditions e.g. defined user name or Windows logon user name.

The matched results display in the listed box, double click any one record will be directed to related log or policy settings

3.3.4 Delete

Administrator can select **File->Delete** to delete computer (group) or user (group). Deleting computer (group) will uninstall the Agents of the selected group or selected computer as well as update the license number.

Deleting user (group) will only remove current basic information.

3.3.5 Rename

Select the computer (group) or user (group) to change name from **File->Rename** to rename.

3.4 Control

Administrator can control the running agents using IP-guard Console, the prerequisite is the agent must be in running status. To be reminded that all controls can only be done in Computer mode but not in User mode.

3.4.1 Notification

IP-guard can send notification to a computer or a group. Select **Control→Notify** to notify the selected computer or group. In **Notify** dialogue box, enter the message and click **Send** to notify the target computer or group.

3.4.2 Lock/Unlock Computer

IP-guard can lock the computer or the whole group of computers to prevent users on the agent computer to use the keyboard and mouse in case of abnormal event happened. Select **Control->Lock Computer** to lock. The locked computer will show that it is locked in its basic information

Select **Control->Unlock** to unlock the computer. The target computer will once again be able to use the mouse and keyboard.

3.4.3 Log Off, Power Down/Restart Computer

Administrator can turn off / log off / restart any running agent computers. Select **Log Of**, **Restart** or **Power Down** from the **Control** menu, he agent will execute the order immediately until the computer re-started or logon again.

3.5 Supplementary Functions

In IP-guard Console, there are some other common functions that often used, the followings introduced the detailed functions and descriptions

3.5.1 Export and Import

Export Data

In IP-guard, the data such as statistics, event logs, policies, instant message contents, emails and asset management all can be exported and saved as HTML/Excel/Text(csv) files.

Export Current Page

In any event logs, right click **Export→Records of Current Page** will export the current page data. By default there are 20 records in each page, administrator can amend the maximum number of records in Console, **Tools→Options→Console Settings→Logs**.

Export All Matched Data

Right click **Export→All Matched Records** will export all records

Export / Import Policy

Only policy control provides Import function. IP-guard facilitates administrator to export/import policies from one server to other servers

Export Function

In any policy settings panels, right click to select **Export/Export Selected/Export All** to save the policies in XML file (see Figure 3.14). If **Exported Selection** option is selected, only the selected policy will be exported and saved.

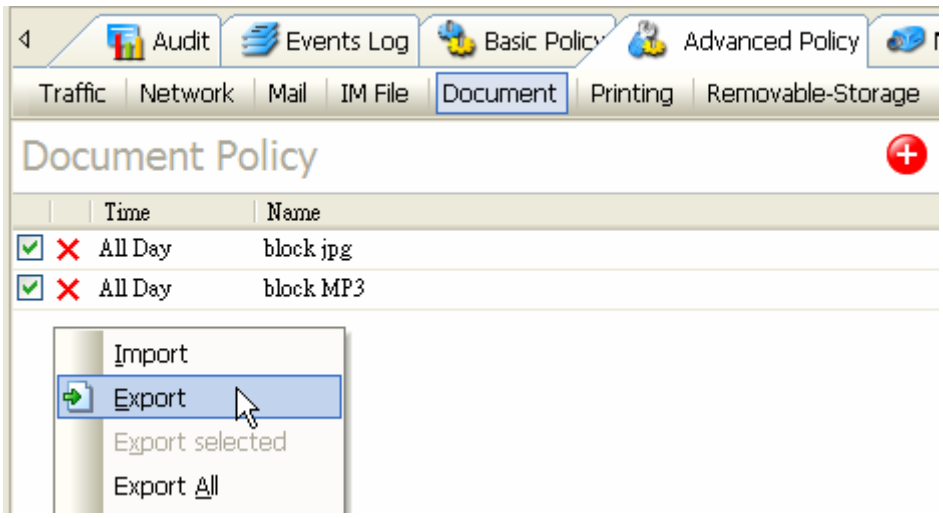


Figure 3.14 Export All Policies

Import function

Select specified computer (group) or user (group) from the Network tree first, right click **Import** in the policy setting panel (see Figure 3.15). The File Open Dialogue will popup, select the related XML file, import process will be started. To take effect on the imported policies, click the button to save the policies (see Figure 3.16)

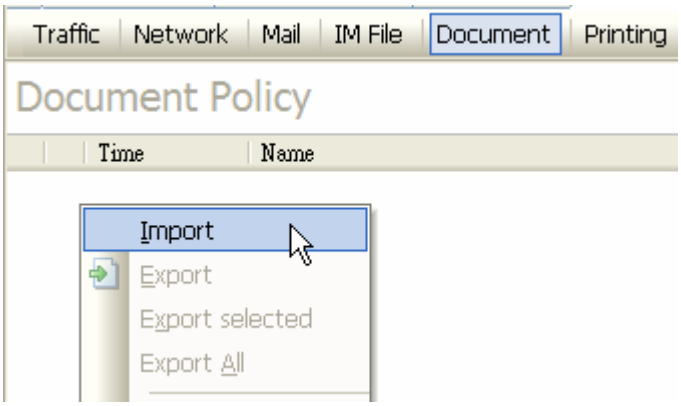


Figure 3.15 Import Policies

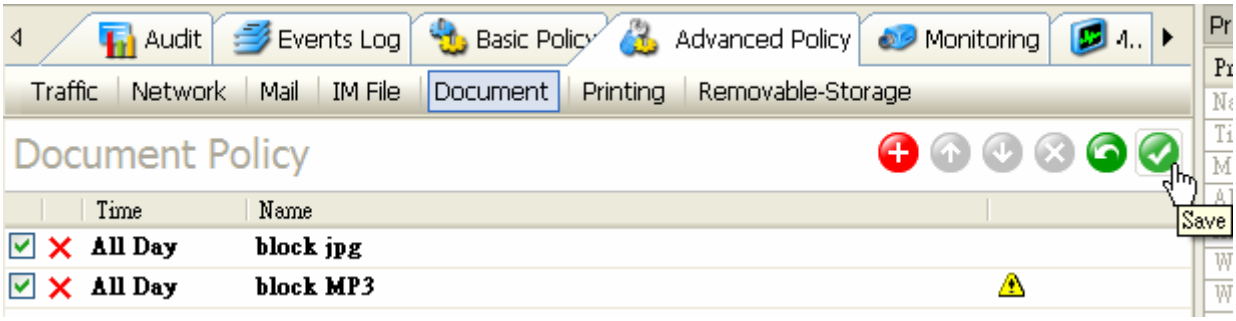


Figure 3.16 Save Imported Policies

[Important]

About Import Policy...
The imported type of policies must be as same as exported one, otherwise, the policies cannot be imported successfully.

3.5.2 Print and Print Preview

All data logs in IP-guard Console can print out. Select **File→Print** to start to print your target data or select **File→Print** Preview to preview the output before printing.

Chapter 4 Statistics

IP-guard assists management people to evaluate staff's working performance according to the collected statistics reports on application usage, Internet browsing and network traffic.

4.1 Application Statistics

Application statistics provide powerful statistical functions to focus on the computer daily operations and application usage to provide detailed records and complete analysis report. The statistical data provides reference to managerial people to assess employees' working behavior.

Select **Statistic → Application** to query the application usage of computer (group) or user (group) in a given period of time. By default, it queries today's statistics of application usage.

The interface of Application Statistics is divided into 4 parts: (1) Computer or User column, (2) Statistical Data Panel, (3) Chart Panel and (4) Search Panel (see Figure 4.1)

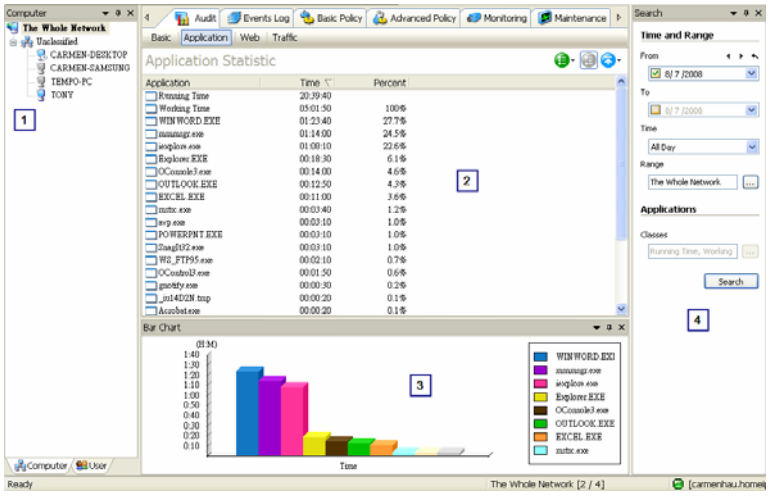


Figure 4.1 Interface of Application Statistics

[Function Button]

	Mode – Administrator can select different application statistic view mode. Options include: **By Class**, **By Name**, **By Detail** or **By Group**
	Expand – In By Class view mode, if an application classes have sub-classes, use this button to expand and view the sub-classes. For group view, expand button can expand the computer group or user group to view the computers or users within the group. This button will turn grey and be disabled in detail view.
	Show – Control number of records to display. Options include All, Top 10, Top 20, and Custom. This button will turn grey and be disabled when selected by class mode and expand.

Table 4.1 Statistics – Functional Buttons

In Application Statistic, the startup time and working time are default collected statistical data. Startup time means that the agent computer starts running after logging to Windows; the working time means the operations of mouse and keyboard controlled by agent computer.

There are 4 modes in Application Statistics:

1. By Class

In this mode, System Administrator can query the statistics by class. The application class can be defined in **Tools → Classes Management → Applications**. Using this mode can facilitate to query defined application usage (Details refer to Chapter 12, Section 12.4.1)

To choose this option, click the **Mode** button and then select **By Class**. By default, it shows all statistics of defined application classes, each record contains the following details:

Class	The name of application class defined in the Application Class Management
Time	The total usage time of that particular application class.
Percent	The total percentage used by particular application class.

Table 4.2 Statistics – By Class

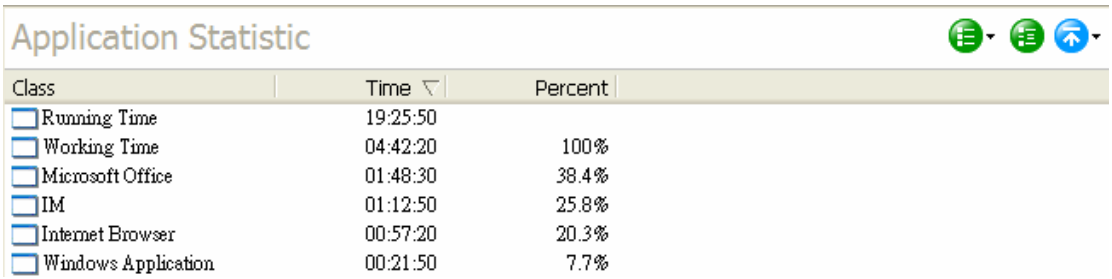


Figure 4.2 Application Statistics – By Class

2. By Name

In this mode, it lists in the order of all statistics of application usage with application executable name, usage of time and its percentage of selected computer (group) or user (group).

To choose this option, click the **Mode** button and then select **By Name**.

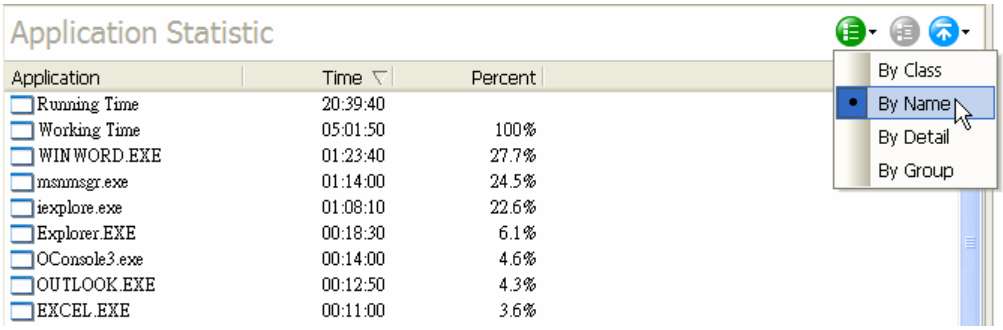


Figure 4.3 Application Statistics – By Name

3. By Detail

In this mode, it listed in the order of the details of application, not by process. For example, there are two different versions of MSN program running in different agents, the process name are the same, called msnmsgr.exe. Using **By Detail mode**, they are counted as two different versions of MSN. However, if using **By Name mode**, the usage time of those two versions will be counted together.

To choose this option, click the **Mode** button and then select **By Detail**.

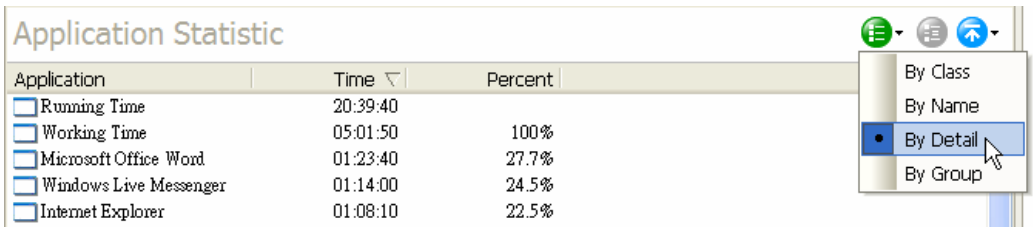


Figure 4.3 Application Statistics – By Detail

4. By Group

In this mode, it analyzes the application and its percentage usage based on selected computer (group) or user (group). By default, the statistical data are working time and running time.

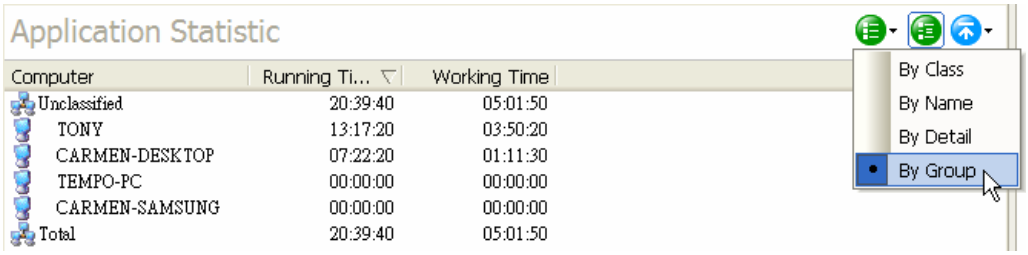


Figure 4.4 Application Statistics – By Group

To query other application classes usage should be selected from **Search Panel → Classes** field and click the button  , the following windows will popup.

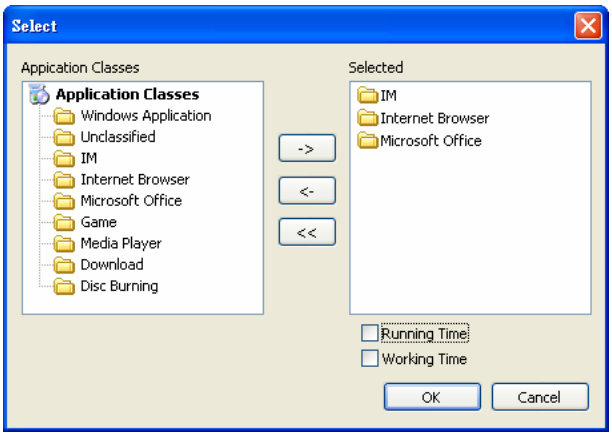


Figure 4.5 Application Classes Select Windows

For example (refer to above figure), to get the statistics of IM and Internet Browser application classes by specified computer (group) and user (group), the method is selecting the target application class from left panel, and click the button -> . Click **OK** to complete the selection. Finally, click the button **Search** to get the result in the Data Panel

Application Statistic

Computer	IM	Internet Browser	Microsoft Office
Unclassified	01:15:20	01:23:00	02:42:10
CARMEN-DESKTOP	00:44:20	00:17:40	00:00:00
TONY	00:31:00	01:05:20	02:42:10
TEMPO-PC	00:00:00	00:00:00	00:00:00
CARMEN-SAMSUNG	00:00:00	00:00:00	00:00:00
Total	01:15:20	01:23:00	02:42:10

Figure 4.6 Application Statistics – By Group by specifying Application Class

Application Statistics not only show the list table, it can also generate charts to present the statistical data. There are two types of charts: Bar Chart and Pie Chart

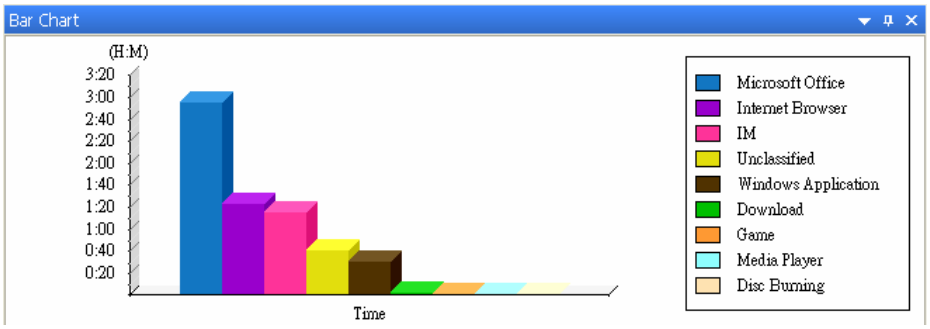


Figure 4.8 Application Statistics – Bar Chart

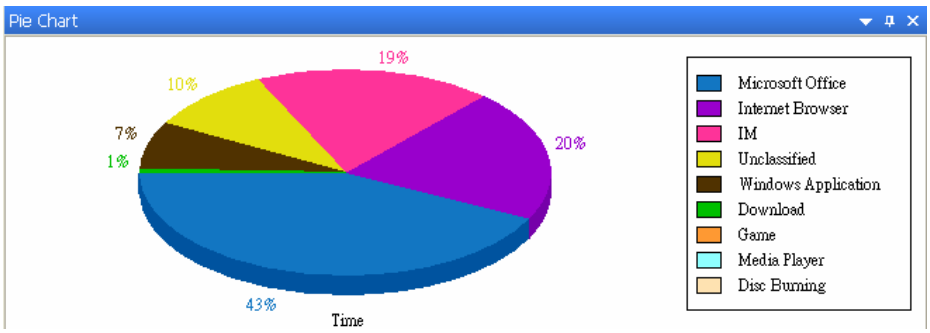


Figure 4.8 Application Statistics – Pie Chart

4.2 Web Statistics

Web statistics provide statistics on users what websites they visited. The statistical data provides reference to easily understand user web browsing behavior.

Select **Statistic → Web** to query the web usage of computer (group) or user (group) in a given period of time.

By default, it queries today's statistics of web usage.

The interface of Web Statistics is divided into 4 parts: (1) Computer or User column, (2) Statistical Data Panel, (3) Chart Panel and (4) Search Panel (see Figure 4.9)

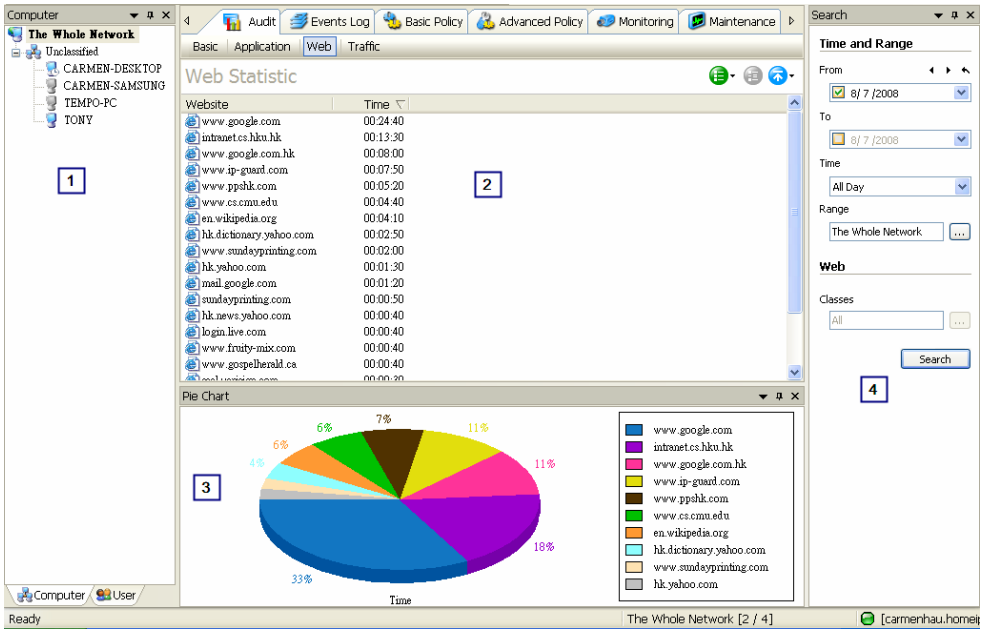


Figure 4.9 Interface of Web Statistics

[Function Button]

	**Mode** – Administrator can select different web statistic view mode. Options include: **By Class**, **By Detail** or **By Group**
	**Expand** – In **By Class** view mode, if a web classes have sub-classes, use this button to expand and view the sub-classes. For group view, expand button can expand the computer group or user group to view the computers or users within the group. This button will turn grey and be disabled in detail view.
	**Show** – Control number of records to display. Options include All, Top 10, Top 20, and Custom. This button will turn grey and be disabled when selected by class mode and expand.

Table 4.3 Web Statistics – Functional Buttons

There are 3 modes in Web Statistics:

1. By Class

In this mode, System Administrator can query the statistics by class. The web class can be defined in **Tools → Classes Management → Web**. Using this mode can facilitate to query defined web usage (Details refer to Chapter 12, Section 12.4.2)

To choose this option, click the **Mode** button and then select **By Class**. By default, it shows all statistics of defined web classes. All websites not classified are grouped into a class called **Unclassified**.

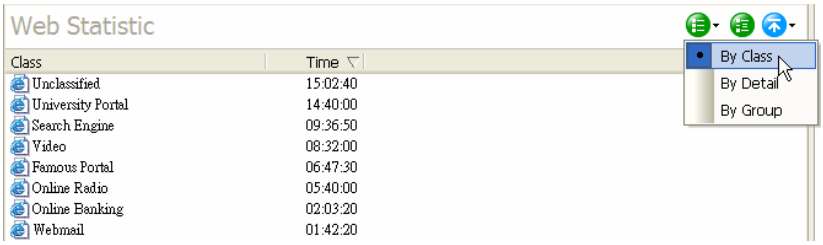


Figure 4.10 Web Statistics – By Class

2. By Detail

In this mode, it listed in the order of all details of website. If the website belongs to one of the web classes, the format of the representation is **Website Identity – Website**. For example, a Website Identity is Google, if www.google.com visited, it listed as **Google – www.google.com**. If none of any web classes it belongs to, it shows the URL directly and analyzed by its domain name.

To choose this option, click the **Mode** button and then select **By Detail**.

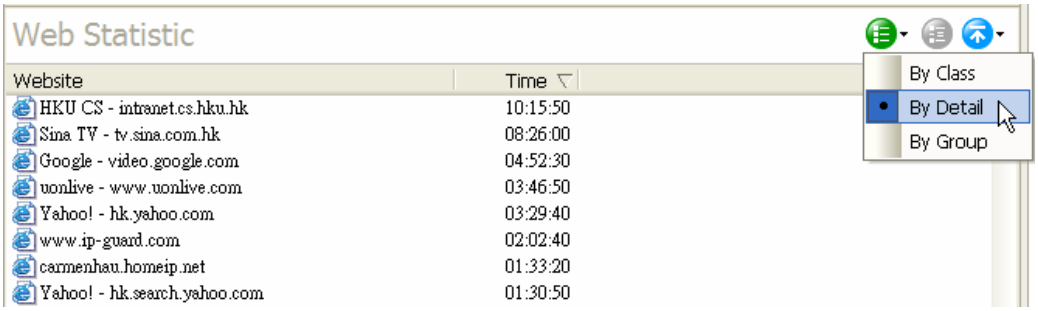


Figure 4.11 Web Statistics – By Detail

3. By Group

In this mode, it analyzes the website and its percentage usage based on selected computer (group) or user (group). By default, all statistical data is listed

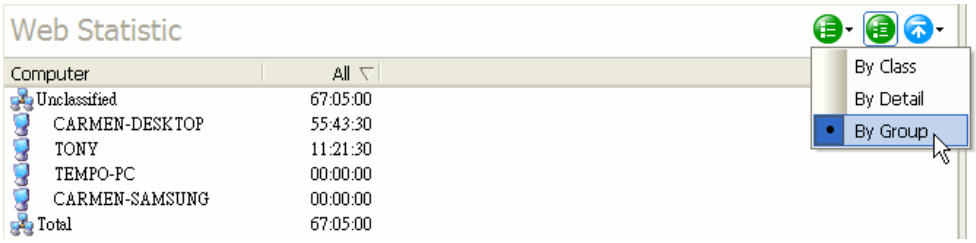


Figure 4.12 Web Statistics – By Group

To query other web classes usage should be selected from **Search Panel → Classes** field and click the button  , the following windows will popup.

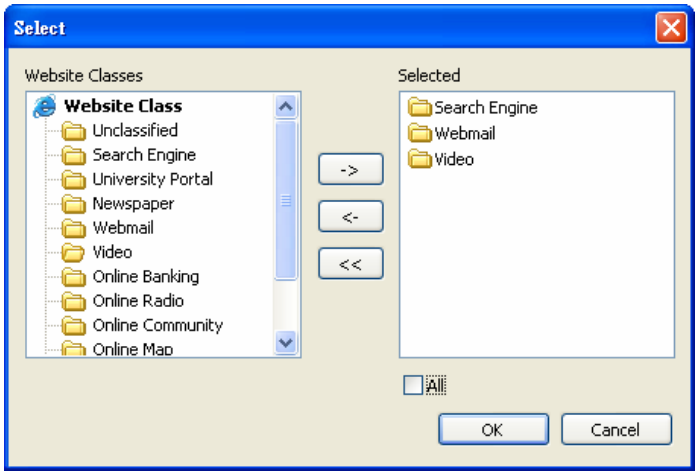
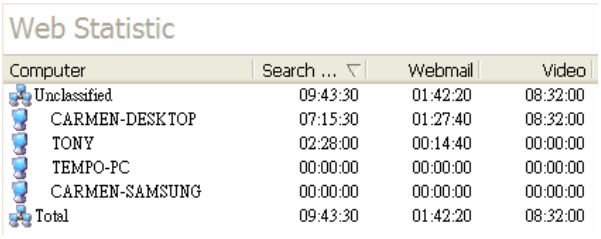


Figure 4.13 Web Statistics Web Classes Selection Windows

For example (refer to above figure), to get the statistics of Search Engine, Webmail and Video web classes by specified computer (group) and user (group), the method is selecting the target web class es from left panel, and click the button  . Click **OK** to complete the selection. Finally, click the button **Search** to get the result in the Data Panel



Computer	Search ...	Webmail	Video
Unclassified	09:43:30	01:42:20	08:32:00
CARMEN-DESKTOP	07:15:30	01:27:40	08:32:00
TONY	02:28:00	00:14:40	00:00:00
TEMPO-PC	00:00:00	00:00:00	00:00:00
CARMEN-SAMSUNG	00:00:00	00:00:00	00:00:00
Total	09:43:30	01:42:20	08:32:00

Figure 4.14 Web Statistics – By Group by specifying Web Classes

Web Statistics not only show the list table, it can also generate charts to present the statistical data. There are two types of charts: Bar Chart and Pie Chart

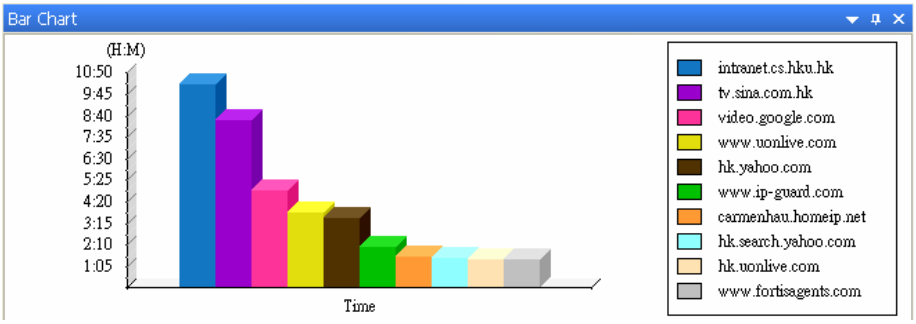


Figure 4.16 Web Statistics – Bar Chart

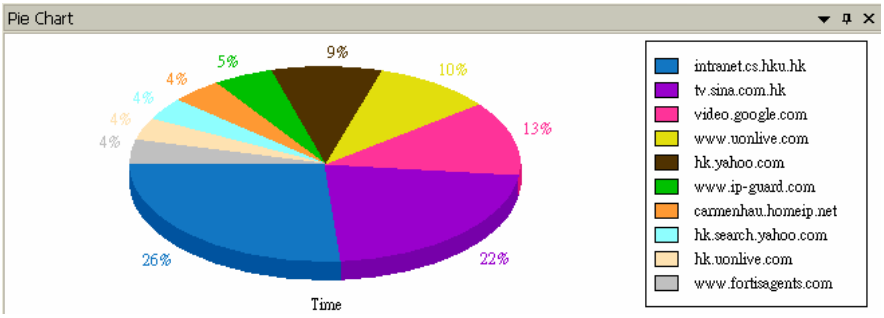


Figure 4.17 Web Statistics – Pie Chart

4.3 Traffic Statistics

The Network Traffic Statistics help Network Administrator to quickly trace the network obstruction problems so that they can make the appropriate response measures to fix the problems. Network traffic statistics include both sides of the communications' network address, ports and bandwidth, such information help Network Administrators to view the current network status.

Select **Statistic → Traffic** to view the use of network traffic.

The interface of Traffic Statistics is divided into 4 parts: (1) Computer or User column, (2) Statistical Data Panel, (3) Chart Panel and (4) Search Panel (see Figure 4.18)

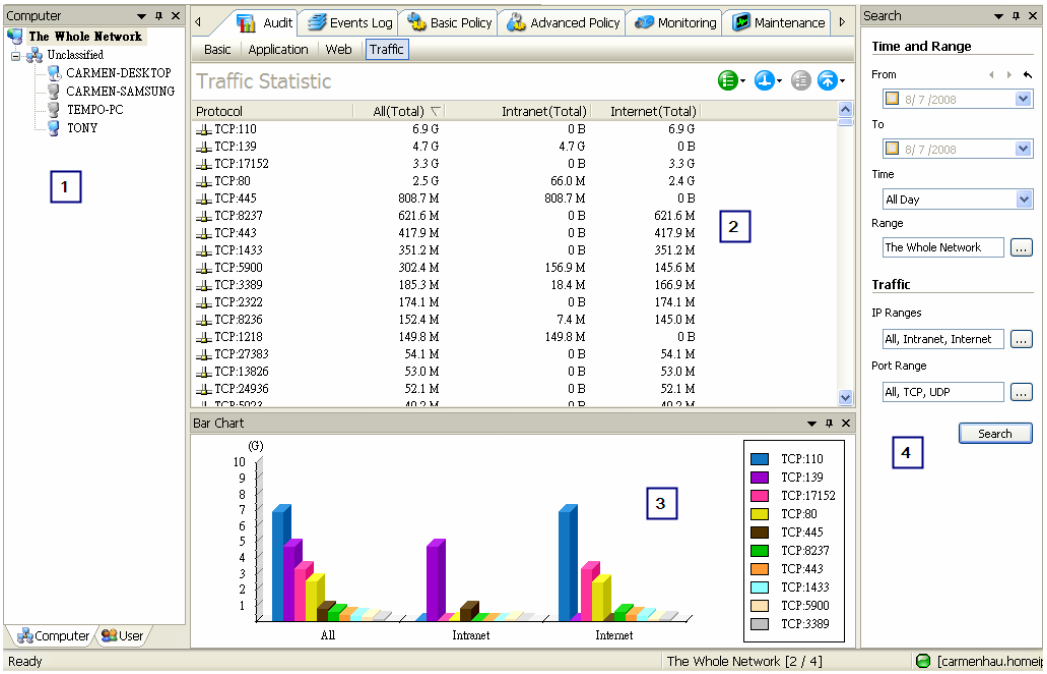


Figure 4.18 Interface of Traffic Statistics

[Function Button]

	**Mode** – Administrator can select different traffic statistics view mode: **By IP**, **By Port**, **By IP Classes**, **By Port Classes**, **By Computer/IP Classes** or **By Computer/Port Classes**
	**Direction** – Traffic directions: Total, Sent or Received
	**Expand** – In by **IP classes** or by **Port classes** view mode, if **IP / Port classes** have sub-classes, use this button to expand and view the sub-classes. In **By Computer/IP classes** view or **By Computer/Port classes** view, expand button can expand the computer group to view the computer detail within the group. This button will turn grey and be disabled in **IP / Port** detail view.
	**Show** – Control number of records to display. Options include All, Top 10, Top 20, and Custom. This button will turn grey and be disabled when selected by class mode and expand.

Table 4.4 Traffic Statistics – Functional Buttons

[Search Conditions]

Date / Time Range	Common Search conditions: Specified start date, end date, time and range
IP Range	Specified remote IP addresses. System Administrator can select the Network IP classes which are defined in **Tools → Classes Management → Network Address** or directly input the IP address in the IP Range field.
Port Range	Specified remote IP ports. System Administrator can select the Network Port classes which are defined in **Tools → Classes Management → Network Port** or directly input the communication protocol with IP port e.g. TCP:139 in the IP Range field. If not specified the protocol, by default it is TCP.

Table 4.5 Traffic Statistics – Search Conditions

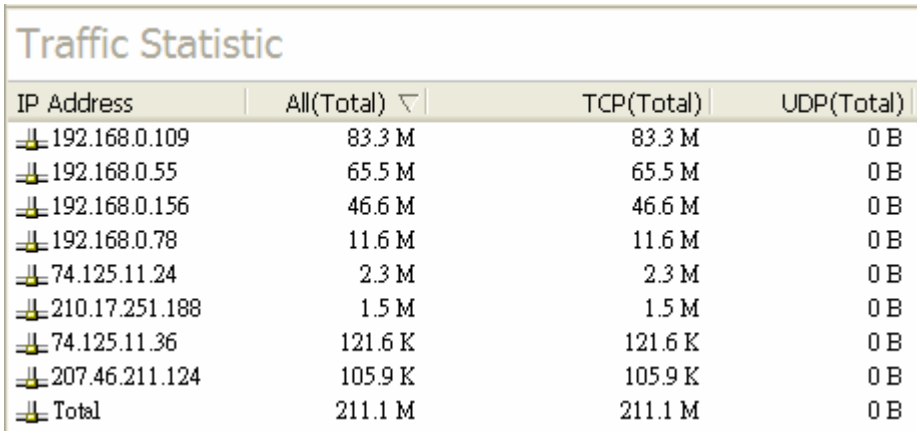
There are 6 modes in Traffic Statistics:

1. **By IP**

List the details of remote IP addresses traffic by selecting computer (group) or user (group). By default, the statistics shows the remote IP address and the corresponding Port/Port Classes traffic statistics: All (total), TCP (total) and UDP (total).

IP Address	This column lists all remote IP address. If IP range is specified from the Search panel, it only lists the specified IP range Select from **Search Panel → IP range** to specify the IP range or input the IP address directly
All (Total)	- It represents the total traffic of all ports. By default, the total traffic of TCP and UDP are also listed. If port range is specified from the Search panel, it only lists all specified range - Select from **Search Panel → Port range** to specify the port range - Click the **Direction** button  to specific the traffic directions: Total, Sent or Received

Table 4.6 Traffic Statistics – By IP



Traffic Statistic

IP Address	All(Total)	TCP(Total)	UDP(Total)
192.168.0.109	83.3 M	83.3 M	0 B
192.168.0.55	65.5 M	65.5 M	0 B
192.168.0.156	46.6 M	46.6 M	0 B
192.168.0.78	11.6 M	11.6 M	0 B
74.125.11.24	2.3 M	2.3 M	0 B
210.17.251.188	1.5 M	1.5 M	0 B
74.125.11.36	121.6 K	121.6 K	0 B
207.46.211.124	105.9 K	105.9 K	0 B
Total	211.1 M	211.1 M	0 B

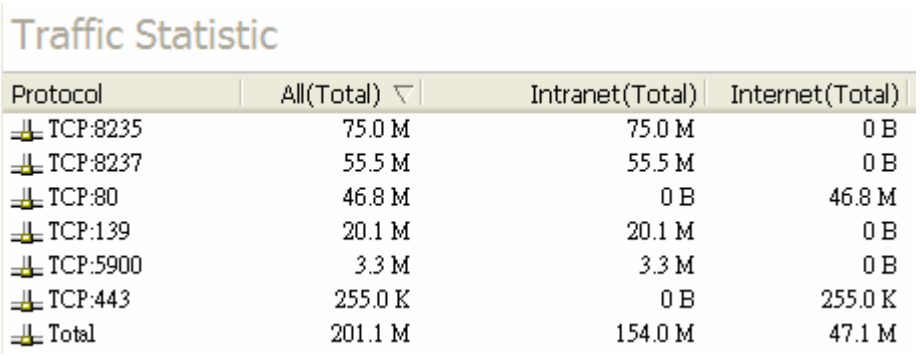
Figure 4.19 Traffic Statistics – By IP

2. By Port

List the details local IP address traffic by selecting computer (group) or user (group). By default, the statistics shows the protocol and port used in local IP address and the corresponding IP/IP Classes traffic statistics: All (total), TCP (total) and UDP (total).

Protocol	This column lists all ports with corresponding protocol e.g. TCP: 80 If Port range is specified from the Search panel, it only lists the specified Port range
All (Total)	- It represents the total traffic of local IP address. By default, the total traffic of Intranet and Internet are also listed. - Select from **Search Panel → IP range** to specify the IP range or input the IP address directly - Click the **Direction** button to specific the traffic directions: Total, Sent or Received

Table 4.7 Traffic Statistics – By Port



Traffic Statistic

Protocol	All(Total)	Intranet(Total)	Internet(Total)
TCP:8235	75.0 M	75.0 M	0 B
TCP:8237	55.5 M	55.5 M	0 B
TCP:80	46.8 M	0 B	46.8 M
TCP:139	20.1 M	20.1 M	0 B
TCP:5900	3.3 M	3.3 M	0 B
TCP:443	255.0 K	0 B	255.0 K
Total	201.1 M	154.0 M	47.1 M

Figure 4.20 Traffic Statistics – By Port

3. By IP Classes

List the details of **IP Classes** traffic by selecting computer (group) or user (group). By default, the statistics shows the **IP Classes** and the corresponding **Port/Port Classes** traffic statistics: All (total), TCP (total) and UDP (total).

Traffic Statistic

IP Address	All(Total)	TCP(Total)	UDP(Total)
All	2.8 G	2.8 G	0 B
Intranet	2.7 G	2.7 G	0 B
Internet	138.9 M	138.9 M	0 B

Figure 4.21 Traffic Statistics – By IP Classes

4. By Port Classes

List the details of **Port Classes** traffic by selecting computer (group) or user (group). By default, the statistics shows the **Port Classes** and the corresponding **IP/IP Classes** traffic statistics: All (total), Intranet (total) and Internet (total).

Traffic Statistic

Protocol	All(Total)	Intranet(Total)	Internet(Total)
TCP	2.8 G	2.7 G	138.9 M
All	2.8 G	2.7 G	138.9 M
UDP	0 B	0 B	0 B

Figure 4.22 Traffic Statistics – By Port Classes

5. By Computer / IP Classes

List the details of **By Computer / IP Classes** traffic by selecting computer (group) or user (group). By default, the statistics shows the **Computer** and the corresponding **IP/IP Classes** traffic statistics: All (total), Intranet (total) and Internet (total).

Traffic Statistic

Computer	All(Total)	Intranet(Total)	Internet(Total)
Fiancial	1.4 G	1.4 G	29.1 M
Unclassified	1.2 G	1.2 G	62.7 M
IT	201.1 M	154.0 M	47.1 M
Total	2.8 G	2.7 G	138.9 M

Figure 4.23 Traffic Statistics – By Computer/IP Classes

6. By Computer / Port Classes

List the details of **By Computer / Port Classes** traffic by selecting computer (group) or user (group). By default, the statistics shows the **Computer** and the corresponding **Port/Port Classes** traffic statistics: All (total), TCP (total) and UDP (total).

Traffic Statistic

Computer	All(Total)	TCP(Total)	UDP(Total)
Fiancial	1.4 G	1.4 G	0 B
Unclassified	1.2 G	1.2 G	0 B
IT	201.1 M	201.1 M	0 B
Total	2.8 G	2.8 G	0 B

Figure 4.24 Traffic Statistics – By Computer/Port Classes

Traffic Statistics not only show the list table, it can also generate charts to present the statistical data. There are two types of charts: Bar Chart and Pie Chart

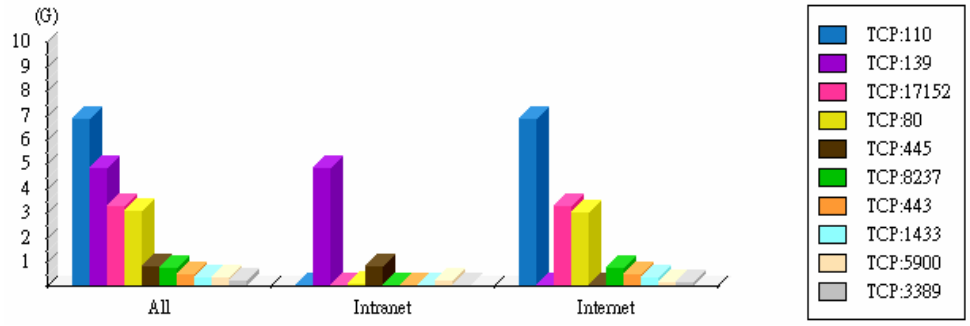


Figure 4.25 Traffic Statistics – Bar Chart

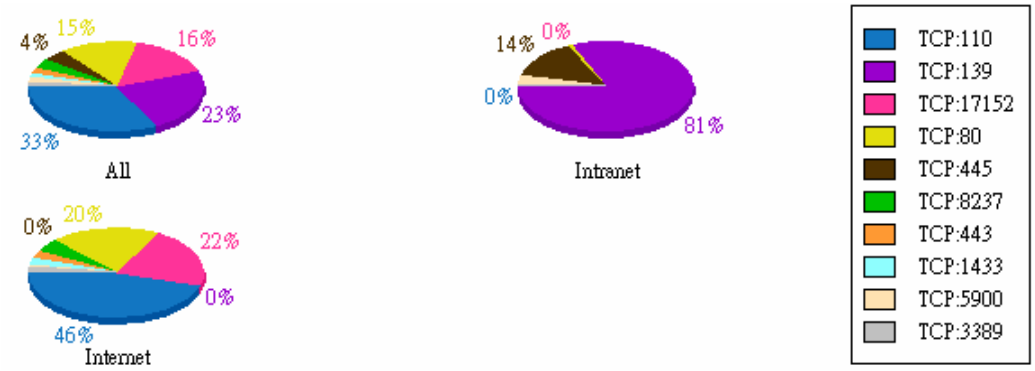


Figure 4.26 Traffic Statistics – Pie Chart

[Important]

About Traffic Statistics...
Traffic statistics can only be applied to computers mode. It does not support in user mode.

Chapter 5 Event Log

IP-guard log the all operation logs from agent computers including user logon, logout, application log, web log, document operation log, shared document log, printing log, removable-storage log, asset changes log etc.

There are some common functions provided in each log, for example, after selecting one of the log records, right click to select Print, Print Preview, Export, Delete, View Screen History and Property.

Common Log Function	
Print / Print Preview	Every page log can print review and print out
Export	Export the current or selected page logs to HTML / CSV / XLS format. There are two options: Records of Current Page and All Matched Records
Delete	Right click to select **Delete** from the log to delete the target log. There are three options: Selected Records, Records of Current Page and All Matched Records
View Screen History	System administrator can view the corresponding screen history of the log. Select one of the log records, right click to select **View Screen History**, the corresponding screen history will display in the viewer. If no Screen Snapshot policy is set, of course no related history can be displayed.
Property	Double click the selected log to view the details of the log

Table 5.1 Common Log Functions

5.1 Basic Event Log

Select **Log→Basic Events**, this basic event log will record the systems' startup/shutdown, login/logoff, dialup, Patch scanning and software distribution related information. Also, the corresponding Time, Computer, User and Description are also recorded. The following table summaries the details of Operating Type:

Operating Type	
Startup / Shutdown	The operating system startup and shutdown status of agent computers
Login / Logoff	Every user login / logoff status
Dialup	Every time when the user dialup, the corresponding action will be logged
Patches	When System administrator requests patches installation, the related patches will be installed automatically, those installation statuses such as Patch scanning and Patch installation will be logged, the details will be showed in the Description column
Deployment	When System administrator create software distribution task, it will be executed on target agent computers. Those tasks will be logged.

Table 5.2 Basic Event Log – Operating Type

Administrator can input time and range, type and description to filter the search result. Input string support wildcard character.

Search Conditions	
Time and Range	Input specified date, time and range to filter the search result
Type	By default it is set to All, also can select specified types: startup/shutdown, login/logoff, Dialup, Patched or Deployment
Description	Input any contents to query the target log, support wildcard input

Table 5.3 Basic Event Log – Search Conditions

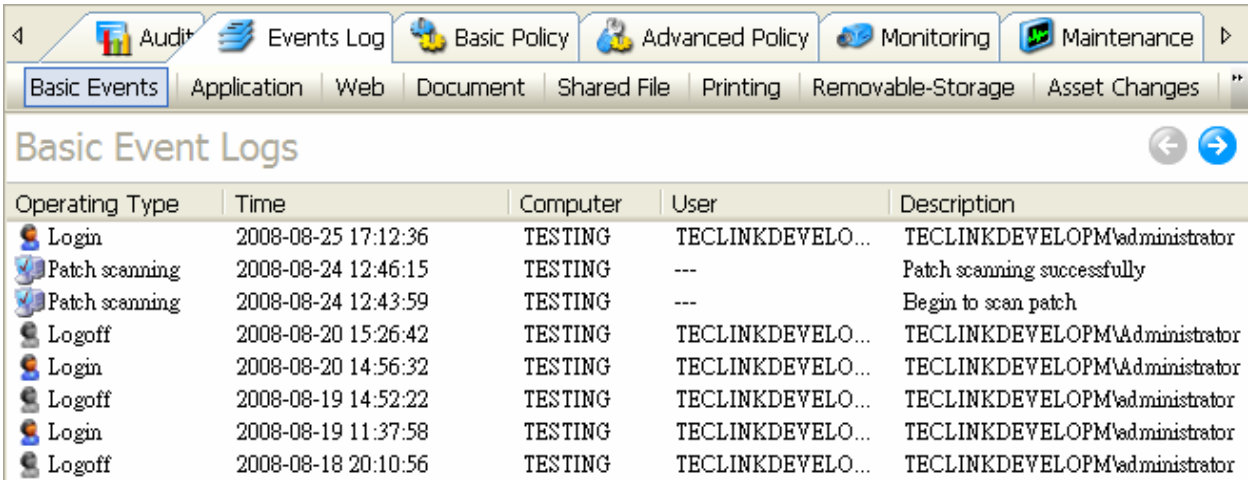


Figure 5.1 Basic Event Log

5.2 Application Log

Select **Log→Applications**, administrator can view all applications start, stop, window change, and title change login, and logoff event.

Log Types	
Start / Stop	Log the status of application start and stop
Windows Changes	When user changes the application, system records the windows changes log
Title Changes	When user uses an application, it may have different windows or titles such as browser

Table 5.4 Application Log – Log Type

☞ **Hints:**

Notes that Window / Title changes are not logged by default, the settings can be changed through **Basic Policy→Event Log** to record window and title changes.

Administrator can input time and range, type in path or window title, and enter specific application or application class to filter the search result. Input string support wildcard character.

Search Conditions	
Path / Title	Input the application path or title for part of query conditions
Application	Input the application name directly or specified the application class for part of query conditions a) input the application name directly System administrator can input the application name directly e.g. qq.exe or *game*.exe b) specified application class Select the button [...] to specify the application class

Table 5.5 Application Log – Search Conditions

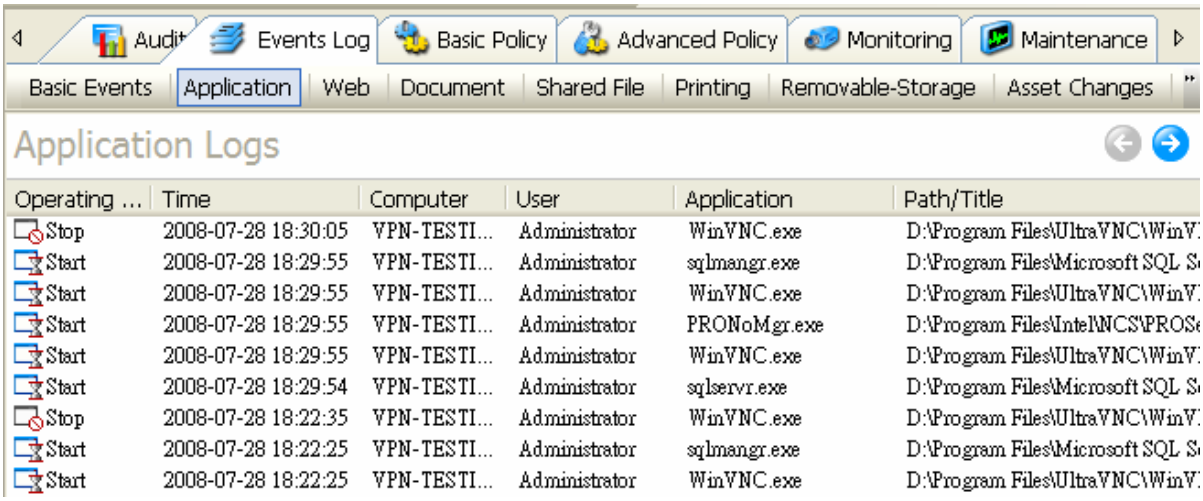


Figure 5.2 Application Logs

5.3 Web Log

Select **Log->Web**, administrator can view the web browsing log. Web log supports different browsers including IE, Firefox, Netscape and Opera etc.

Log Contents	
Caption	Website caption
URL	Detailed URL

Table 5.6 Web Log – Log Contents

☞ **Hints:**

Notes that by selecting one of the web logs, right click to select **Open URL** to open the web page directly from the system default browser.

Administrator can input time and range, enter specific URL or web class, and Window Title to filter the search result. Input string support wildcard character.

Search Conditions	
Time and Range	Input specified date, time and range to filter the search result
URL	Input the target URL or web class, supports wildcard input.
Window Title	Input the target windows title e.g. *mail* to query all related webmail log

Table 5.7 Web Log –Search Condition

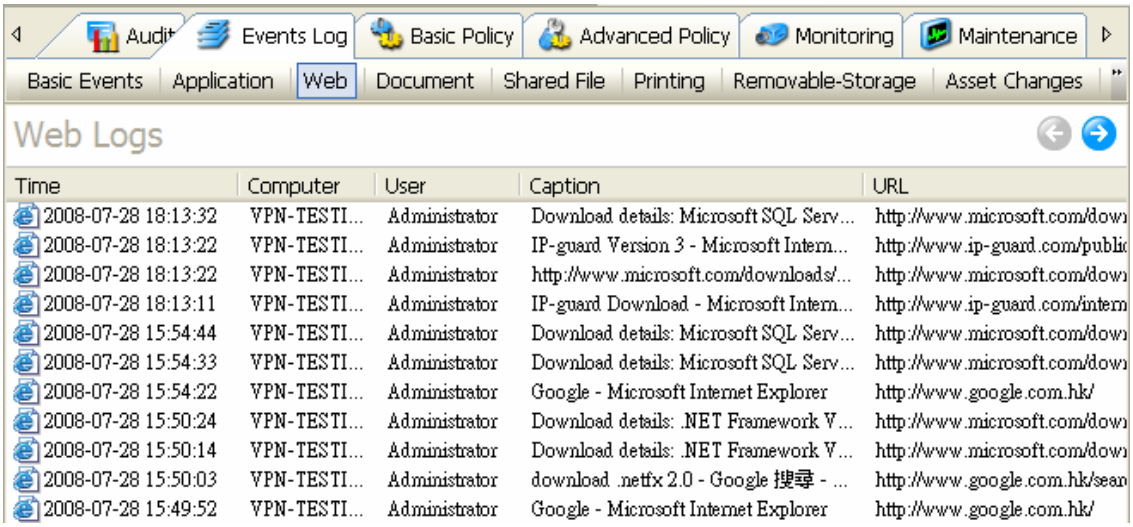


Figure 5.3 Web Logs

5.4 Document Operation Log

Select **Log→Documents** to view all document operation logs of the agents.

Document Operation Types
Include create, access, modify, rename, copy, move, delete, restore and upload/send

Table 5.8 Document Operation Log – Document Operation Types

Disk types
Support Fixed, Floppy, CD-ROM, Removable and Network

Table 5.9 Document Operation Log – Disk Types

Log Contents	
The document operation log contents include document operation Type, Time, Computer, User, Source Filename, File size, Path, Disk Type, Application and Caption	
Source Filename	The file operated by agent computer user
Path	The details of file operation path. When user copies, moves, rename the file, the details of source and destination of the file path are also displayed.
Disk Type	The location of the document which may be on the fixed disk, network drive, removable storage or CD-ROM. When user copies, moves, rename the file, the details of source and destination of the disk types are also displayed.
Application	The application used to operate the file
Caption	The caption of the document operations

Table 5.10 Document Operation Log – Log Contents

Backup Document Log
In the document and IM File policies, when these policies are invoked with document backup. The backup document should be retrieved here (i.e. Document Operation Log). This icon represents the log with the backup file inside. Double click the log, a button **Copy** should be placed in the dialogue windows. Click this button to retrieve the backup document directly.

Table 5.11 Document Operation Log – Backup Document Log

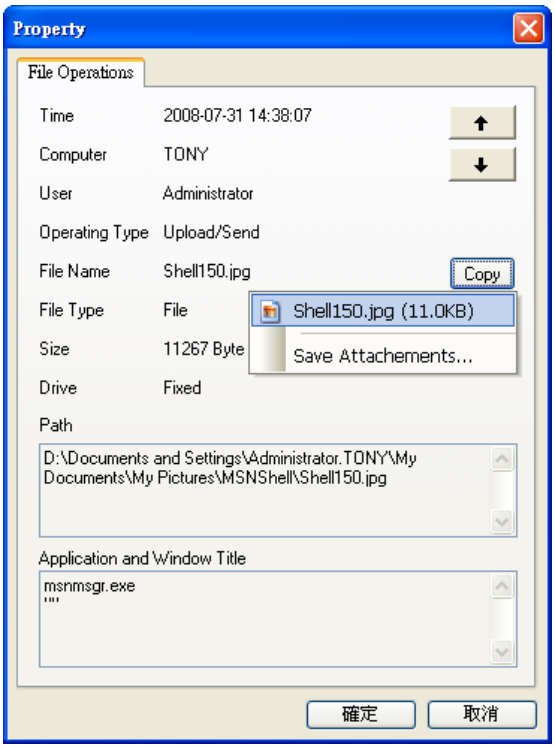
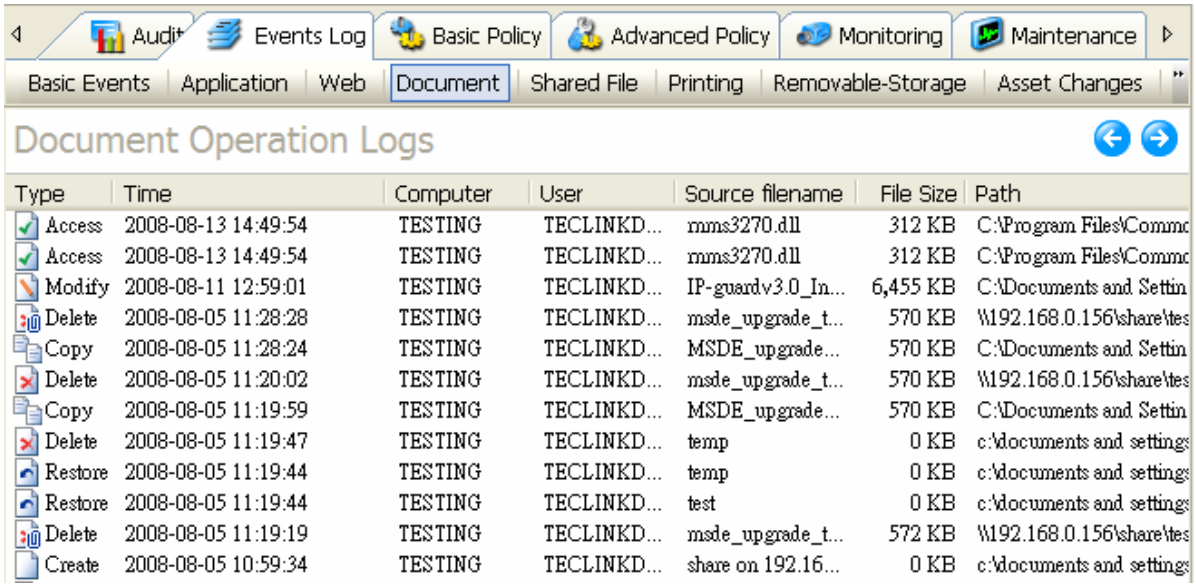


Figure 5.4 Document Operation Log – Property

Administrator can input time and range, select operating type, drive where the document is located, file name, file size range, and application that opened the file to filter the search result. Input string support wildcard character.

Search Conditions	
Time and Range	Input specified date, time and range to filter the search result
Operating Type	By default, it is set to All. Specified type can be selected from the drop-down menu including Create, Copy, Move, Rename, Restore, Delete, Access, Modify and Upload/Send
Drive	By default, it is set to All. Specified drive can be selected from the drop-down menu including Fixed, Floppy, CDROM, Removable and Network
Filename	Based on the filename to filter the query. Support wildcard input
Size	Specify the file size to query the target document log
Application	Input the application name directly or specified the application class for part of query conditions c) input the application name directly System administrator can input the application name directly e.g. qq.exe or *game*.exe d) specified application class Select the button ... to specify the application class
Has Backup	Check this Has Backup box to query the document log with backup only

Table 5.12 Document Operation Log – Search Conditions



Type	Time	Computer	User	Source filename	File Size	Path
Access	2008-08-13 14:49:54	TESTING	TECLINKD...	mms3270.dll	312 KB	C:\Program Files\Commc
Access	2008-08-13 14:49:54	TESTING	TECLINKD...	mms3270.dll	312 KB	C:\Program Files\Commc
Modify	2008-08-11 12:59:01	TESTING	TECLINKD...	IP-guardv3.0_In...	6,455 KB	C:\Documents and Settin
Delete	2008-08-05 11:28:28	TESTING	TECLINKD...	msde_upgrade_t...	570 KB	\\192.168.0.156\share\tes
Copy	2008-08-05 11:28:24	TESTING	TECLINKD...	MSDE_upgrade...	570 KB	C:\Documents and Settin
Delete	2008-08-05 11:20:02	TESTING	TECLINKD...	msde_upgrade_t...	570 KB	\\192.168.0.156\share\tes
Copy	2008-08-05 11:19:59	TESTING	TECLINKD...	MSDE_upgrade...	570 KB	C:\Documents and Settin
Delete	2008-08-05 11:19:47	TESTING	TECLINKD...	temp	0 KB	c:\documents and settings
Restore	2008-08-05 11:19:44	TESTING	TECLINKD...	temp	0 KB	c:\documents and settings
Restore	2008-08-05 11:19:44	TESTING	TECLINKD...	test	0 KB	c:\documents and settings
Delete	2008-08-05 11:19:19	TESTING	TECLINKD...	msde_upgrade_t...	572 KB	\\192.168.0.156\share\tes
Create	2008-08-05 10:59:34	TESTING	TECLINKD...	share on 192.16...	0 KB	c:\documents and settings

Figure 5.5 Document Operation Log

5.5 Shared File Log

Select **Log→Shares**, administrator can view log of shared files in the agent that had been operated by others. Logged operations include create, rename, modify, and delete.

Shared File Operation Types
Include create, modify, rename, copy, delete BUT access, copy and move operations not supported

Table 5.13 Shared File Log – Operating Types

Log Contents	
The shared file log contents include document operation Type, Time, Computer, Remote Host, Source Filename and Path	
Remote Host	Remote Computers' IP address
Source Filename	The file operated by agent computer user
Path	The details of file operation path.

Table 5.14 Shared File Log – Log Contents

Administrator can input time and range, select operating type, file name, and remote computer name or IP address to filter the search result. Input string support wildcard character.

Search Conditions	
Time and Range	Input specified date, time and range to filter the search result
Operating Type	By default, it is set to All. Specified type can be selected from the drop-down menu including Create, Rename, Delete and Modify
Name	Based on the filename to filter the query. Support wildcard input
Remote IP / Name	Specify the remote IP or computer name to filter the query

Table 5.15 Shared File Log – Search Conditions

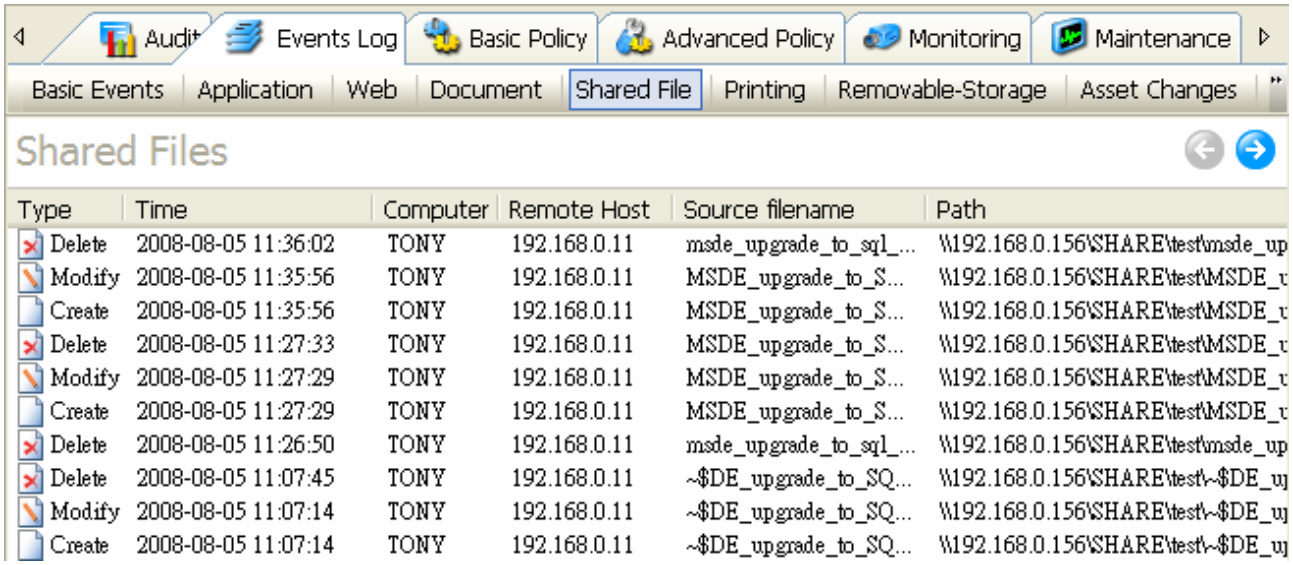


Figure 5.6 Shared Files Log

5.6 Printing Log

Select **Log→Printing**, administrator can view the printing log of the agent including usage of local printer, shared printer, network printer, and virtual printer.

Log Contents	
The printing log contents include Printer Type, Time, Computer, User, Printing Task, Printer Name, Pages, Caption and Application	
Printing Task	Printed document name
Printer Name	The printer used to print out the document
Pages	The total number of pages
Caption	The windows caption when printing
Application	The application used to operate and print out the document

Table 5.16 Printing Log – Log Contents

Administrator can input time and range, printer type, printer name, computer name, printing task title, page size range, and application to print to filter the search result. Input string support wildcard character.

Search Conditions	
Time and Range	Input specified date, time and range to filter the search result
Printer Type	By default, it is set to All. Specified printer type can be selected from the drop-down menu including Local, Shared, Network and Virtual printers
Printer	Specify the printer to filter the query to get the statistics to access the printer usage
Computer	Specify the remote IP or computer name to filter the query
Task	Specify the document name. Support wildcard input
Pages	Specify the pages to filter the query to monitor the printer usage
Application	Input the application name directly or specified the application class for part of query

	conditions e) input the application name directly System administrator can input the application name directly e.g. qq.exe or *game*.exe f) specified application class Select the button … to specify the application class

Table 5.16 Printing Log – Search Conditions

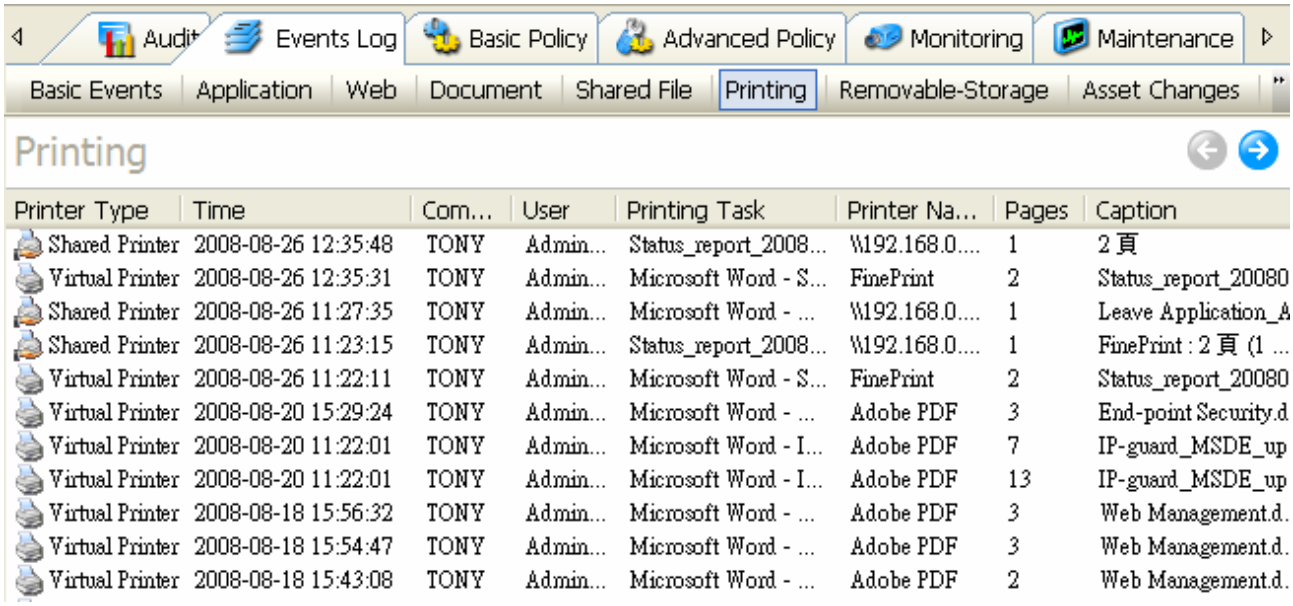


Figure 5.7 Printing Log

5.7 Removable-storage Log

Select **Log→Removable-storage** to view the log of all agent computers' removable storage plug-in and plug-off actions.

Log Contents	
The removable-storage log contents include Type, Time, Computer, User, Disk Type, Volume ID, Description and Volume Label.	
Volume ID	The volume ID is an unique ID of every removable-storage device, this data can also be found in Removable-storage class.
Description	The details information of the removable-storage device
Volume Label	The name of removable drive

Table 5.17 Removable-storage Log – Log Contents

Administrator can input time and range, removable storage name and operation type to filter the search result. Input string support wildcard character.

Search Conditions	
Time and Range	Input specified date, time and range to filter the search result
Removable Storage	Specified the removable-storage class for part of query conditions. Select the button

	… to specify the application class
Operation Type	By default, it is set to All. Specified removable-storage type can be selected from the drop-down menu including Plug-in and Plug-out

Table 5.18 Removable-storage Log – Search Conditions

5.8 Assets Change Log

Select **Log→Asset Changes**, administrator can view the asset change log of hardware and software including add, delete, and change.

Log Contents	
The asset log contents include Operating Type, Time, Computer, Type and Description	
Operating Type	Add, Delete and Change of the asset
Type	Identify the change is Software or Hardware
Description	The information of asset changes

Table 5.18 Assets Change Log – Log Contents

Administrator can input time and range and asset description to filter the search result. Input string support wildcard character.

Search Conditions	
Time and Range	Input specified date, time and range to filter the search result
Type	By default, it is set to All. Specified removable-storage type can be selected from the drop-down menu including Hardware Changes and Software Changes
Operation Type	By default, it is set to All. Specified removable-storage type can be selected from the drop-down menu including Add, Delete or Change
Description	Specify the asset description to filter the query. Support wildcard input.

Table 5.19 Assets Change Log –Search Conditions

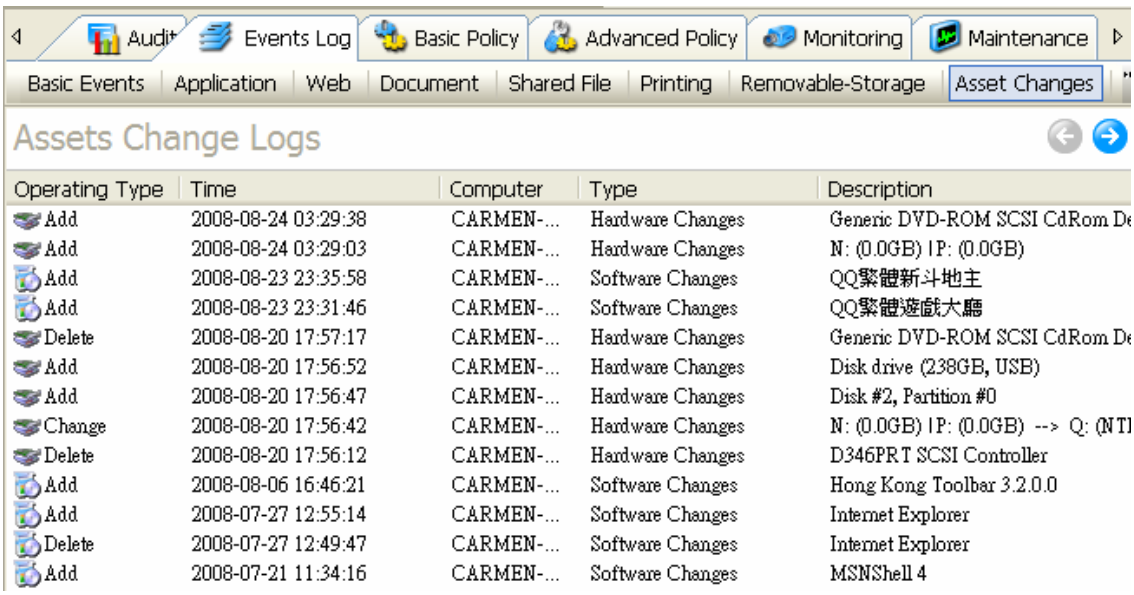


Figure 5.8 Assets Change Log

5.9 Policy Log

Select **Log→Policies**, administrator can view the log trigger by policy setting.

Log Contents	
The policy log contents include Alert Level, Time, Computer, User, Policy and Description	
Alert Level	There are three alert levels: Low, Important and Critical. The alert level settings can be done in each policy
Policy	The corresponding policy triggered by agent.
Description	The information of triggered policy

Table 5.20 Policy Log – Log Contents

Administrator can input time and range, lowest alert level, policy type, and content to filter the search result. Input string support wildcard character.

Search Conditions	
Time and Range	Input specified date, time and range to filter the search result
Lowest Alert Level	By default, it is set to All. Specified alert level can be selected from the drop-down menu including Low, Important and Critical
Policy Type	By default, it is set to All. Specified policy type can be selected from the drop-down menu
Content	Specify the policy description to filter the query. Support wildcard input.

Table 5.21 Policy Log – Search Conditions

5.10 System Log

Select **Log→System**, administrator can view the server start and stop status, illegal intrusion, and agent connection errors.

Administrator can input time and range and content to filter the search result. Input string support wildcard character.

☞ **Hints:**

In case of any agents cannot connect to IP-guard server, System administrator can check this System log to find out the reasons.

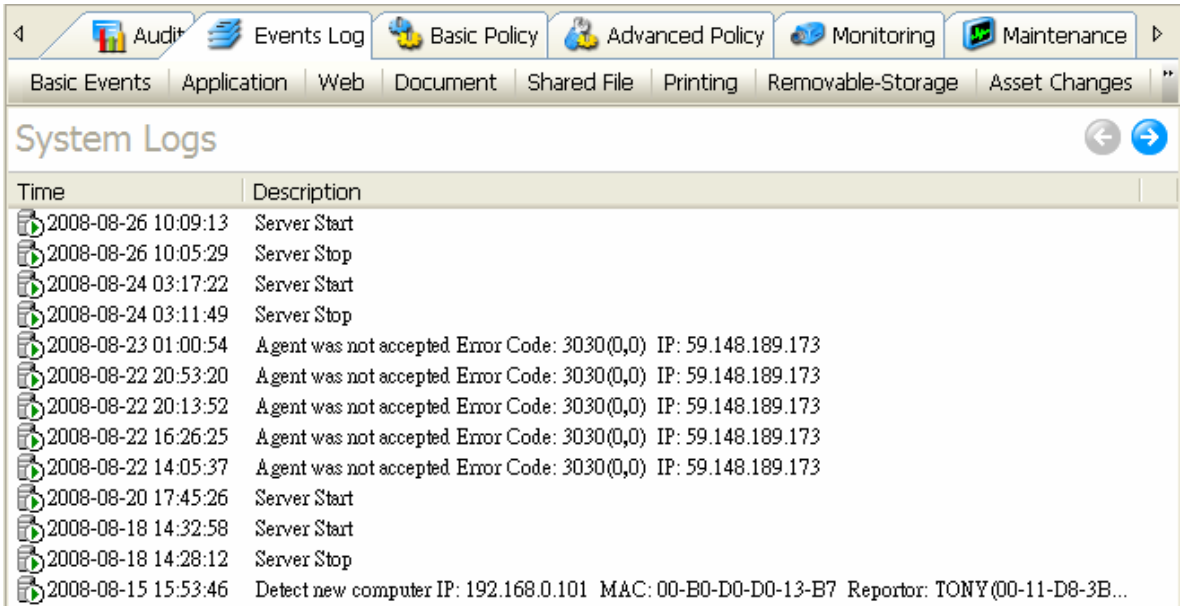


Figure 5.9 System Logs

Chapter 6 Policy

6.1 Policy Introduction

Administrator can limit the use of computer and network resource on agent computer by setting policies to control staffs' computer usage and improve productivity.

Common Policy Properties

Name	This is user-defined name to descript the policy. It is irrelevant to the actual function of the policy. When adding a new policy, the system will add a default name to the policy and administrator can change it later
Time	This is time range that the policy is effective. It can be self-defined time type. Time types are set in **Tools→Time Types**. If no suitable time type available, select **Custom** and set the time range from the popup time matrix.
Mode	After satisfying the policy conditions, there are some modes can be selected to be executed: **Block**, **Allow**, **Inaction** and **Ignore**. **Allow**: Allow to perform an operation. According to the hierarchy (user policy has higher priority than computer policy; self policy has higher priority than group priority; policy on top has higher priority than the policy below), when a policy found in higher priority, it will be executed and the policies in lower priority will be ignored. **Block**: Block an operation. According to the hierarchy, policy in higher priority is executed and the policies below it are ignored. **Inaction**: Neither allows or block an operation, but it can trigger events such as warning or alert. According to the policy matching principal, once the current Inaction policy completed, the following policies will not be executed. For example, the first policy is setting the mode for USB device as Inaction and the second policy is prohibiting USB device. When USB device is plugged in, the first policy matched. Since the mode is Inaction, it will not be blocked but the following second policy will not be matched. **Ignore**: Neither allows or block an operation, but it can still trigger events such as warning or alert. According to the policy matching principle, system continues to search the following related policies. For example, the first policy is setting all *.doc with Ignore mode and alert; the second policy is prohibiting copy *.doc files. When accessing the doc files, the first policy matched (i.e. alert popup) and then the following second policy will also be matched too (i.e. determine the accessing action is copy or not. If it is copy, action prohibited.
Action	While the policy is executing, there are 3 types of actions are also taking action: **alert**, **warning**, and **lock computer**. **Alert**: When a matched policy with alert option is executed, the console can receive a popup message to alert administrator. The popup alert can be set from **Tools→Option→Real Time**

	Alert→Popup Bubble to set rather to have popup alert bubble. There are three types of alert: **Low**, **Important**, and **Critical**. Meanwhile, the server will record the alerts and can be viewed from policy log or alert log. **Warning**: When a matched policy with warning option is executed, a dialog box will pop up on the agent computer. The content of the warning message can be set in each policy. **Lock computer**: When a matched policy with lock computer option is executed, the agent computer will be locked. To unlock, select from toolbar **Control→Unlock** or highlight the target agent from the network tree and then right click to select from the menu **Control → Unlock**
Expiring Time	By default, the expiry date setting is **Always**. In other words, the policy always keeps active, never expired. A policy will always be effective before its expiry date. Click … button to set the expiry date. In the **Setting** windows, check the **Apply** and input the expiry time. The system does not allow user to set expire date earlier than the current date. If the policy is expired, the fonts in the policy will be displayed in dark grey and the **Expiring Time** will be displayed in red.
Only Offline	When no communications between server and agent is over 3 minutes, it indicates that agent is in offline status. The policy will only be effective when console determines the agent is in offline status. When should apply this option is: System administrator may apply different policies for notebook users when it is for business trip, office & home uses or in case the network cable plug off.

Table 6.1 Common Policy Properties

Priority Matching for Policy

Policy adopted mechanism is similar to Firewall, each goal can be combined from a number of policies and then matched in accordance with their relationships. At the same time, different computers (group) or users (group) inherit their parents' policies.

Function of Policy Buttons


New, click this button to add a new policy


Up, move up selected policy


Down, move down selected policy


Delete, delete selected policy


Restore, cancel new added policy or any modified settings


Save, click this button to save all new added or modified settings


Indicates that the policy mode is "**allow**"


Indicates that the policy mode is "**block**"


Indicates that the policy mode is "**ignore**"

	Indication that the policy mode is “**inaction**”
	Indicates that the policy with **alert** setting
	Indicates that the policy with **warning** setting
	Indicates that policy with **lock computer** setting
	Indicates that policy with **expiring time** setting

Table 6.2 Policy Functional Buttons

 **[Important]**

Key Concept: Priority Matching for Policy

- System administrator can apply policies to the whole network, group, computer and user levels. According to the hierarchical mechanism, their accordance of priorities is: **User Policy > Computer Policy > Group Policy > The Whole Network Policy**

- The inherited policy is indicated as light green color . The property fields related to string input are all supported by wildcard (each string up to 3 wildcards) and multiple inputs separated by **;** and **,**

6.2 Basic Policy

Through the Basic policy can regulate the computer operation rights, also restrict the end users not easily to change the system settings to prevent malicious destroy and strengthen the security.

To make the Basic policy work is to amend the system registry. Basic policy and Device policy are different from other policies, they are state keeping policy, not a real-time invoked policy.

Basic policy supports: Control Panel, Computers Management, System, Network, IP/MAC Binding and ActiveX controls

Control Panel	
Control Panel	All Control Panel's functions
Modified Display Properties	Restrict users to change the theme, desktop, screen saver and appearance
Add printers	Restrict user to add printers
Delete printers	Restrict user to delete printers
Fast switching user in XP	Restricted in Windows XP only

Computers Management	
Device Manager	Restrict user to use Device Manager
Disk Management	Restrict user to use Disk Management
Local users and groups	Restrict user to use Local users and groups
Service Management	Restrict user to use Service Management
Other computer Managements	Restrict user to use: Event Viewer, Performance Logs and Alerts and Shared Folders which located in Computers Management

System	
Task Manager	Restrict user to use Task Manager
Regedit	Restrict user to use Regedit
CMD	Restrict user to use CMD. For Windows 98, it is **command**, others are **cmd**
"Run" in registry	If the mode is **block** for this option, the process under "Run" will not be run when OS is starting up. **Log off or restart is required for effective**
"RunOnce" in registry	"RunOnce" means that the process only run once when OS is starting up, it will not be run again in the next startup. If the mode is block for this option, the process under "RunOnce" will not be run. **Log off or restart is required for effective**.

Network	
Modify Network Property	Restrict user to modify the network property. The button **Properties** will be disable in the LAN Status windows
Display "Network Places"	If the mode is **block**, My Network Places will be hidden. **Log off or restart is required for effective**
Modify Internet Options	Restrict user to modify Internet Options settings
Default Netshare	If the mode is **block**, the default Netshare will be blocked
Netshare	If the mode is **block**, the user cannot share folders or files

Add Netshare	If the mode is **block**, the user is not allowed to add Netshare

IP/MAC Binding	
Change IP/MAC Property	- Using this option to prohibit user to change the IP settings. Once the prohibited policy is set, the current settings of IP/MAC are saved. If any changes found, it will be resumed to reserved IP/MAC settings. - if required to change IP, the prohibited policy should be deleted first

ActiveX	
Chat ActiveX	Restrict user to use chat ActiveX
Media ActiveX	Restrict user to use Media ActiveX. Generally this kind of ActiveX is applied for playing music or video on Internet. Prohibit this option to stop user listening or watching online media
Game ActiveX	Some online games may require installing its ActiveX. Prohibit this option to stop user playing online game
Flash ActiveX	This ActiveX is required for playing FLASH. Prohibit this option to make the FLASH file cannot be played properly

Others	
PrintScreen keystroke	To block the use of PrintScenne Keystroke
System Restore	To prevent user to restore system back from agent to non-agent state. Using this option to prohibit the system restore function
Windows Automatic Updates	To block the function of the use Windows Automatic Updates

Table 6.3 Basic Policy

Basic Policy: Example 1

Requirements:

IP settings cannot be changed by end-user. However, it should be allowed when the computer is out of office for business trip.

Policy (1): Add a policy at **The Whole Network** level to **block Change IP/MAC Property**

Policy (2): Add another policy at the target **computer (group)** level to **allow Change IP/MAC Property** with option **Only offline** checked

Result:

According to the policy matching mechanism, the second policy (2) should have higher priority. So, the second policy will be matched first – when the computer determined as offline status, the policy (2) will be invoked and the user should be able to change the IP settings. However, if the computer determined as online status, obviously the conditions specified in policy (2) not satisfied, then another policy (1) will continue be matched. As the condition satisfied, policy (1) is invoked, the user should not be able to change the IP settings.

[Important]

Basic Policy: Functions Only effective for Computer (group) settings

The following functions are only effective for Computer (group) settings: **Change IP/MAC Property, System Restore and Netshare**

6.3 Device Control Policy

The device control policies support the followings: Storage, Communication Device, Dial, USB Device, Network Device and other devices.

Storage	
Floppy	Floppy Drive Control, Cannot use floppy if it is prohibited
CDROM	DVD/CD-ROM Drive Control
Burning Device	The burning disks action, but the device still can read
Tape	Tape drive Control
Moveable Device	Includes USB Flash drive, removable drive, memory stick, smart card, MO and ZIP drive control But not includes the device with IDE, SCSI and SATA interface

Communication Device	
COM	COM Ports Control
LTP	LTP Ports Control
USB Controller	USB Controller Control
SCSI Controller	SCSI Controller Control
1394 Controller	1394 Controller Control
Infrared	Infrared device Control
PCMCIA	PCMCIA Card Control
Bluetooth	Bluetooth device Control
MODEM	Modem device Control
Direct Lines	Direct connection control between two computers using USB cable , COM port or Serial cables

Dial	
Dial-up Connection	Dial-up Connection Control

USB Device	
USB Keyboard	USB Keyboard Control
USB Mouse	USB Mouse Control
USB Modem	USB Modem Control
USB Image Device	USB Image Device Control such as Webcam, Digital Camera and Scanner
USB CDROM	USB CDROM Control
USB Storage	USB Storage Control
USB Hard disk	USB Hard disk Control
USB LAN Adapter	USB LAN Adapter Control
Other USB Devices	Control other USB devices not mentioned as above

Network Devices	
Wireless LAN Adapter	Wireless LAN Adapter Control

PnP Adapter (USB, PCMCIA)	
Virtual LAN Adapter	Virtual LAN Adapter Control

Others	
Audio	Audio, video and game controller control
Virtual CDROM	Virtual CDROM Drive Control
Any new devices	Any new devices plug-in. if the mode is block, all new devices cannot be used

Table 6.4 Device Policy

Device Control Policy: Example 1

Requirements:

Some companies' policies not allow staff listening music or playing online game during office hours. In this case, System administrator can set a policy to prohibit the use of Audio

Policy (1): add a policy to **block Audio** in **Device Policy** and set the effective **time** is **Working Time**.

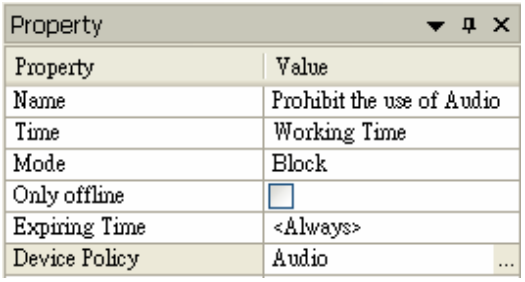


Figure 6.1 Device Policy – Example 1 Property

Device Control Policy: Example 2

Requirements:

To prevent some important files leakage, System administrator can set a policy to prohibit the use of Burning devices, removable device

Policy (1): add a policy to **block** some **Storage** (**Floppy**, **CDROM** and **Moveable** Device), **Communication** (**Bluetooth** as File transfer between local computer and Mobile Phone/PDA may be done through Bluetooth) and **USB** devices (**USB Storage** and **USB Hard disk**) and set the effective **time** as **All Day**

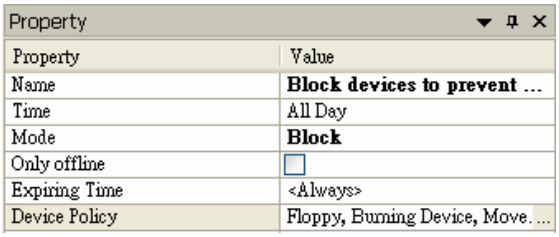


Figure 6.2 Device Policy – Example 2 Property

6.4 Application Policy

Many Enterprises prohibit their staff to install their own application software such as BT, chatting and online games software. Application policy control can limit the use of unwanted applications.

To add a policy, by default, the application is <All>. There are two methods to specify the application:

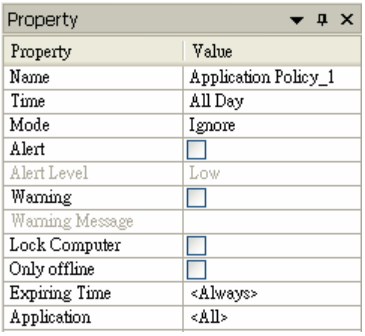


Figure 6.3 Application Policy

1. **Direct Input Application Name**

   In the Application Setting windows, click the button  to input the application name directly e.g. thunder.exe. If the user changes the application name to thunder123.exe, it makes the policy not effective anymore because the input only matched with a string. To avoid this problem, use the following method 2.

2. **Select from Application Class**

   In the Application Setting windows, click the button  and the Application Class Selection windows popup. Check the application classes you want to control. If the mode is block, even the user changes the application name later, the policy is still effective. (How to customize the Application Class please refer to Chapter 12.4.1)

Caution:

Application Policy Warning

Prohibit all applications will cause many processes terminated immediately once the policy applied. Warning message will be given before decided to block all applications.

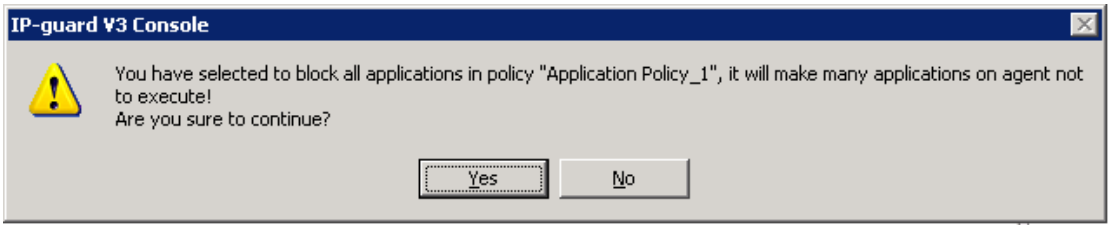


Figure 6.4 Application Policy Warning

6.5 Web Policy

Web Policy effectively controls user to access websites. System administrator can set the web policies to control user to access some prohibited websites.

There are two methods to specify the website:

1. **Direct Input**

   In the Web Setting windows, click the button  to input either a complete URL e.g. www.google.com or wildcard input e.g. *mail*, *game* etc

2. **Select from Web Classes**

   In the Web Setting windows, click the button  and the Web Class Selection windows popup. Check the web classes you want to control. (How to customize the Web Class please refer to Chapter 12.4.2)

Web Policy Example

Requirement:

To control user not access prohibited websites, System administrator can set a web policy to prohibit some websites or only allow accessing specified website. The following policies only allow accessing specified websites.

Policy (1): Add a policy to **block <All>** websites first

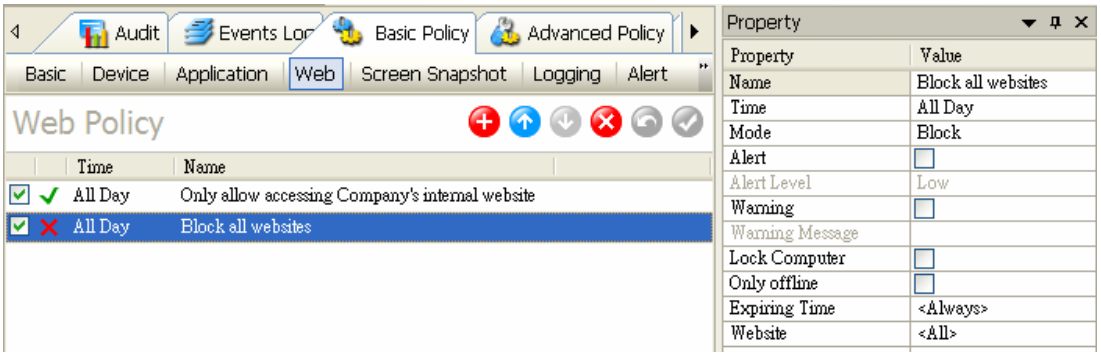


Figure 6.5 Web Policy – Example 1: 1st Policy

Policy (2): Add another policy to **allow** specified (e.g. defined **internal** web class) website

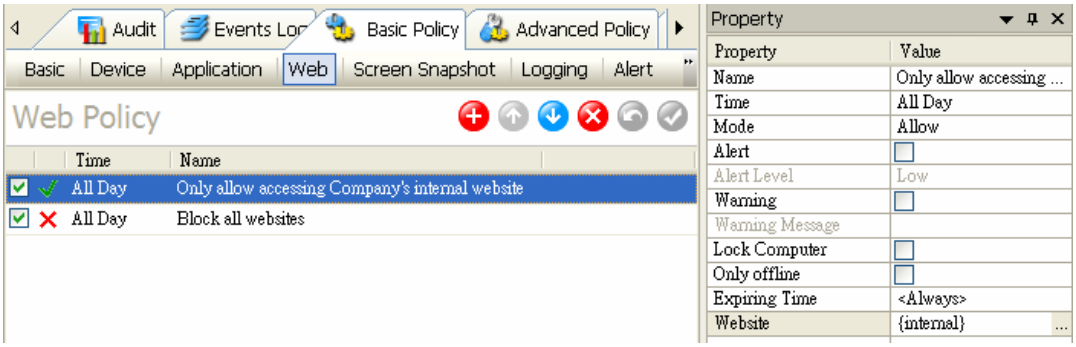


Figure 6.6 Web Policy – Example 1: 2nd Policy

6.6 Screen Snapshot Policy

Screen snapshot function can record all operations behavior in agent computers. By default, system would not record anything as the data size is quite large, System administrator can base on their needs to set a policy to record the screen snapshot.

Policy Properties:

Mode	Record or Not Record
Application	By default, it is <All>. It means all screen snapshot will be recorded based on the interval setting. However, if only required to capture specified applications e.g. Outlook, IM applications, here the System administrator can select the target applications.
Interval (Sec)	By default, the interval setting is 15 seconds. It means system will take a snapshot every 15 seconds. The valid interval range is from 1 to 999 and only enabled under **Record** mode.

Table 6.5 Screen Snapshot Policy Properties

Screen Snapshot Policy Example

Requirements:

Only capture some important applications such as OUTLOOK and IM applications used by end-users

Policy (1): Add a policy to **record** specified applications **{Email}** and **{IM}** with interval settings **2 seconds**

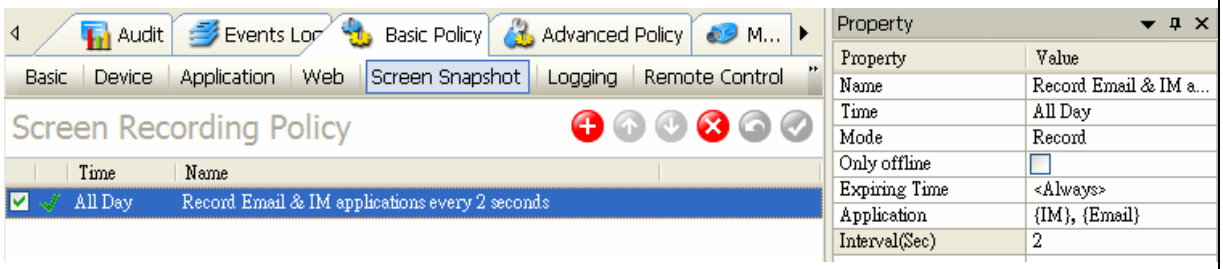


Figure 6.7 Screen Snapshot – Policy Example

[Important]

Be careful the interval setting and available hard disk storage space

- The smaller the interval is set, the larger data size of the screen snapshot history. System administrator should estimate the total size of snapshot and prepare the sufficient hard disk storage space to save the snapshot history.

- Typical reference: The data size is about **42MB** for one agent with Interval setting (all applications) **15s** running **8 hours per day**

6.7 Logging Policy

By default, system has a preset policy to log all logs except Windows Title. Depends on different Enterprises requirements, System administrator can add a policy to uncheck some logs that are not require to log.

Policy Properties:

Mode		Record or Not Record
Startup/Shutdown		Startup/Shutdown log (found in Basic Event log)
Login/Logoff		Login/Logoff log (found in Basic Event log)
Dial		Dial log (found in Basic Event log)
Policy Control		Policy alert log
Hardware Changes		Hardware changes log
Software Changes		Software changes log
Application		Application usage log. System administrator can set a policy to not record application usage log
	Visible Window	It means the application with windows
	Application	System administrator can specify applications, only the specified applications will be logged. The defined application classes can be applied here Supports wildcard input.
Window Title Change		By default, this is not recorded. System administrator can set a policy to log the changes based on different applications (optional)
	Application	System administrator can specify applications, only the specified applications with window title changes will be logged. The defined application classes can be applied here Supports wildcard input.
Web		Web browsing log. System administrator can set a policy to not record web browsing log
	Website	Input the website manually, support wildcard input. The defined web classes can be applied here
Document		Document log. System administrator can select to record or not record certain document type logs to make sure that all logs are useful for future tracing.
	Disk Type	Includes: Fixed, Floppy, CDROM, Removable, Network and unknown disk types. For example, set a policy to not record any file operations on fixed disk
	File Name	Set to record or not record specified filename. Supports wildcard input e.g. not record *.txt ；*.log
	Application	Application for file operations
Printing		Printing log
	Printer Type	Select to record or not record specified printer types
	Application	Application for file operations
Shared Files		Shared files log
	File Name	Shared file name. Support wildcard input.
	IP Range	IP Range for remote access agents' shared files. System administrator can set a range to not record those IP ranges' access operations.
Mail		Log the email contents. Control policies can be set to record or not record the email
	Sender	Email sender address. Supports wildcard input.
	Recipients	Email recipient address. Supports wildcard input.

	Mail Size (>=KB)	If it is set, it means if email is over the specified size will not be logged
	Not Record Attachment	This option only enabled under the mode **Record**. If it is checked, the email attachments will not be logged. In the Console (Monitoring → Mail), the properties of email will tell you if it has attachments, however, cannot be retrieved.
Instant Message		The instant message conversation contents. System administrator can select which IM applications are targeted to log
Application Statistics		Application usage data
Web Statistics		Web browsing data
Traffic Statistics		Network Traffic data

Table 6.6 Logging Policy Properties

Logging Policy Example

Requirement:

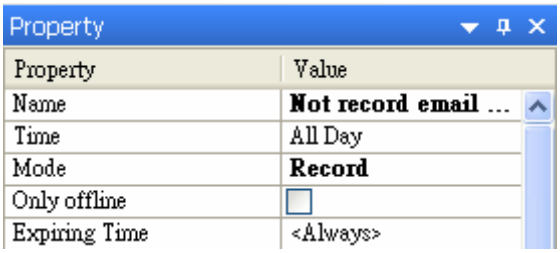
Only log all incoming and outing emails without attachments

Policy (1): Add a logging policy to not record email attachments.

Policy Name: **Not record email attachments**

Mode: **Record**

Mail, Send, Receive and Not Record Attachment: **checked**



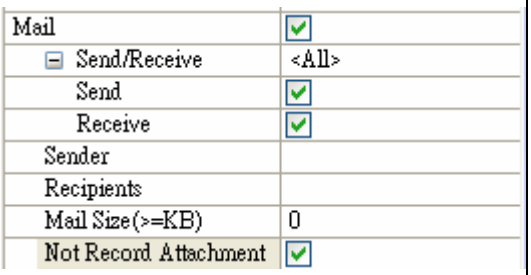


Figure 6.8 Logging Policy – Policy Example

6.8 Remote Control Policy

With remote control policy, we can control the agent computers that can be controlled remotely or not.

There are two controls in Remote Control Policy: **Remote Control** and **Remote File Transfer**

Policy Properties:

Remote Control	This option is only enabled under the mode **Allow**. If checked, it represents that all remote control access rights must be granted by agent side. If not checked, it represents that the remote control access right can be granted by agent or using pre-defined password methods to process the remote control
Manager Name	Target to control the logging on System administrator e.g. can limit some administrator that cannot remote control specified agents. Administrator accounts can be created from **Tools → Accounts…**
Console IP address	Limit the Console within specified IP range to process remote control actions. If the input is .0.0.0.0 – 255.255.255.255, or blank, or invalid IP range, all are treated as all IP address and using <All> to represent.
Console Name	Limit the Console with specified Computer Name to process remote control action.

Table 6.7 Remote Control Policy Properties

Notices that the Manager Name, Console IP address and Console Name support symbol **;** ***** and **,** as separator to allow multiple settings

6.9 Alert Policy

Alert policy is used to monitor the changes from hardware, software and other system settings, any changes system will give alert to System administrator in real time. This facilities the System administrator to understand the real time situation of each computer in the network and make appropriate measures to increase the maintainability.

Alert Policy includes the following alert function: Hardware change, Plug in, Plug off, Plug in Storage Device, Plug off storage Device, Plug in communication device, Plug off communication device, Software changes, System service change, Startup change, System time change, Computer name change and Network configuration change

Policy Properties:

Hardware change	Any hardware installed or removed alert
Plug in	External devices plug-in alert, also record the device name
Plug off	External devices plug-off alert
Plug in storage device	External storage device plug-in alert, also record the device name
Plug off storage device	External storage device plug-off alert
Plug in communication device	External communication device plug in alert, also record the device name
Plug off communication device	External communication device plug off alert
Software changes	Any software installed or removed alert
System service change	Any system services installed or removed alert
Startup change	Any system startup tasks added, deleted or changes alert
System time change	Any System time changes alert
Computer name change	Any computer name changes alert
Network configuration change	Any network configuration changes alert

Table 6.8 Alert Policy Properties

6.10 Bandwidth Policy

Traffic policy is used to control the network bandwidth to avoid malicious use causing the network congestion. Also, the bandwidth can also be controlled based on the specified network port.

Note that traffic policy is only effective for Computer (group) but not for User (group).

Policy Properties:

IP Range	Set the Remote IP address range. By default, it is set <All>. System administrator can add the specified IP range manually or selected from defined Network Address class
Port Range	By default, it is set <All>, the default settings include TCP:0-65535; UDP: 0-65535; ICMP. System administration can add the specified Port range manually or selected from defined Network Ports class.
Direction	The network bandwidth direction. Traffic (Sent) means from agent to remote computer, vice versa. Total Bandwidth = Traffic (Sent) + Traffic (Received)
Limited Speed	To limit the bandwidth speed, unit is KB/s. This is only enabled under **Limited Traffic** mode

Table 6.9 Traffic Policy Properties

If the mode is **Limited Traffic** with specified IP range, port range and direction which is over the limited speed, the agent will be temporarily stop to download or upload until the speed is lower than the specified limited speed.

If the mode is **Ignore** with no other actions specified, the limited speed has no effective. If the IP range, port range are set; and the user actions such as **Alert**, **Warning** or **Lock Computer** are specified; when the speed is over, those actions will be invoked but the speed will not be limited.

Traffic Policy: Example 1

Requirements:

Set a bandwidth policy to control the Internet traffic

Policy (1): Add a **traffic policy** to control the traffic

Policy Name: **Limit the agent traffic**

Mode: **Limited Traffic**

IP range: **Internet**

IP port: **All**

Direction: **Traffic**

Limited Speed: **20** k/s

Traffic Policy: Example 2

Requirement:

Set a bandwidth policy to prohibit FTP download

Policy (1): Add a traffic policy to prohibit FTP download

Policy Name: **Prohibit FTP download**

Mode: **Limited Traffic**

IP range: **All**

IP port: **TCP:21**

Direction: **Traffic**

Limited Speed: **0** k/s

6.11 Network Policy

Network policy can effectively control the communications between agent computers and other illegal computers, also, some malicious network ports or download ports can be blocked to prevent the virus attack.

Notes that network policy is only effective for Computer (group) but not User (group)

Policy Properties:

Direction			3 options: **Both**, **Out** or **In** Outbound and inbound relative to the agent computer i.e. if the agent computer takes the initiative to connect other computers, it represents outbound
Port Range			By default, it is set <All>, the default settings include TCP:0-65535; UDP: 0-65535; ICMP. System administration can add the specified Port range manually or selected from defined Network Ports class.
IP Range			Set the Remote IP address range. By default, it is set <All>. System administrator can add the specified IP range manually or selected from defined Network Address class
Remote is Agent			Determine the remote connection computer is agent or not. The following options are only enabled when this option is checked
	Belong to the same group		The same group means the current agent belonging group, here not included the parent group or the following subgroups
	Belong to the selected group		The selected group means the control between agents and selected group agents. The following 2 options (**Group of agent** and **Include subgroup**) are only enabled if this option is checked.
		Group of agent	Specify the belonging group of remote computers. The following option (**Include subgroup**)is only enabled if this is specified.
		Include subgroup	Check this option to specify to include subgroup or not

Table 6.10 Network Policy Properties

Network Policy: Example 1

Requirements:

To prohibit user accessing website and FTP download

Policy (1): Add a **Network policy** to block the ports 80 and 21

Policy Name: **Block the ports 80 and 21**

Mode: **Block**

IP port: **TCP:80, TCP:21**

IP range: **All**

Network Policy: Example 2

Requirements:

In the Enterprise, there are some important departments which may have many sensitive data. However, to facilitate the staff workflow, they may use net share to share the working files. In this case, how to protect these departments' shared resources away from other departments' illegal access

Policy (1): Add a **Network policy** to block the IP range Intranet first

Policy Name: **Block all intranet communications**

Mode: **Block**

IP port: **All**

IP range: **{Intranet}**

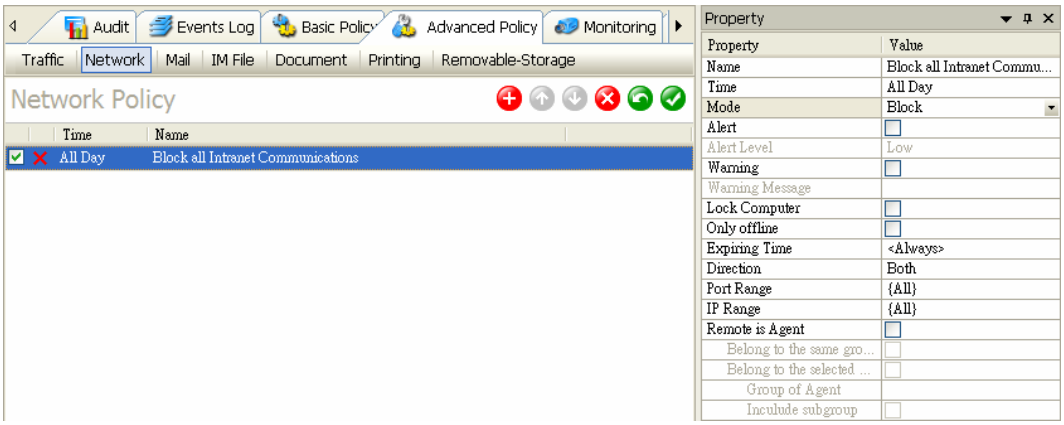


Figure 6.9 Network Policy – Policy Example 1: 1st policy

Policy (2): Add a **Network policy** to **allow remote is agent** + **Belong to the same group**

Policy Name: **Allow communicating with the remote is agent & belong to the same group**

Mode: **Allow**

IP Port: **All**

IP Range: **All**

Remote is Agent: **Checked**

Belong to the same group: **Checked**

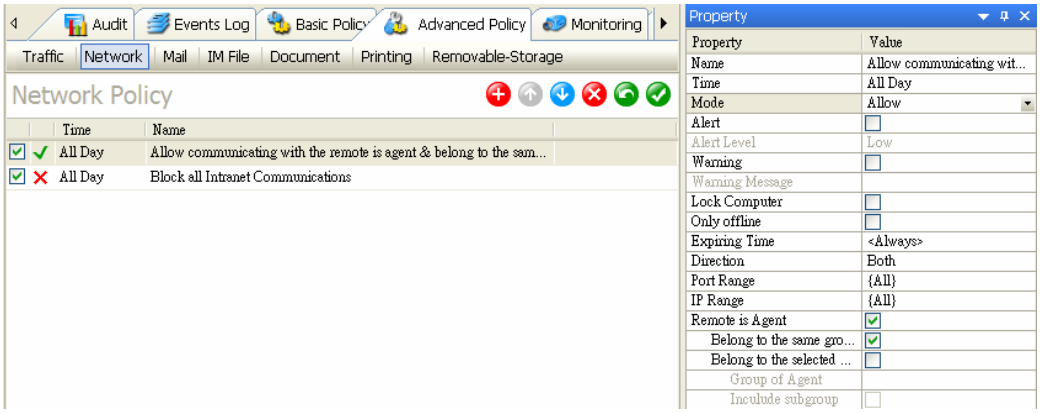


Figure 6.10 Network Policy – Policy Example 1: 2nd policy

Network Policy: Example 3

In practice, the Network policy can combine with the use of Intrusion Detection to prevent external/illegal computers communicating with internal computers

For the enterprise computers installed with agent, network policy should be set to allow only communicating remote is agent. This policy prevents some external computers accessing the internal enterprise computers.

For the enterprise computers not installed with agent, System administrator can **enable** the **Intrusion Blocking** function with set some specified computers as **Protected**. This function will block all communications between **Illegal** (all other external computers are treated as **illegal** which are not listed in the Intrusion Detection windows) and **Protected** computers. Details of Intrusion Detection function please refer to Section 10.

6.12 Mail Policy

Mail policy is used to prevent Enterprise internal information/data leakage through sending email.

Mail policy is used to control outgoing email but cannot control incoming email. Also, IP-guard cannot control webmail and Lotus emails whatever is incoming or outgoing.

Notes that mail policy is only effective for computer (group) but not user (group)

Policy Properties

From		Control the sender email address. Support wildcard and multiple inputs, use **,** and **;** as separators
To		Control the recipients' email address including CC and BCC email addresses. Input rules are same as Sender
Subject		Control the email subject. Input rules are same as Sender
Has attachments		Control the email with/without attachments. If this option is checked, it means the control is only effective for email with attachment. If this option is unchecked, it means the control is effective for all emails whatever the email has attachments or not.
	Attachment	Control the email with specified attachment name. Input rules are same as Sender
	Mail size (>=)	Control the email with specified size. By default, it is set to 0 which represents all. Input the mail size with >= value for conditional control

Table 6.11 Mail Policy Properties

Mail Policy: Example 1

Requirements:

Some enterprises may limit the sender, only allow staff using internal email account to send email, others will be prohibited

Policy (1): Add a **Mail policy** to block all emails

Policy Name: **Block all emails**

Mode: **Block**

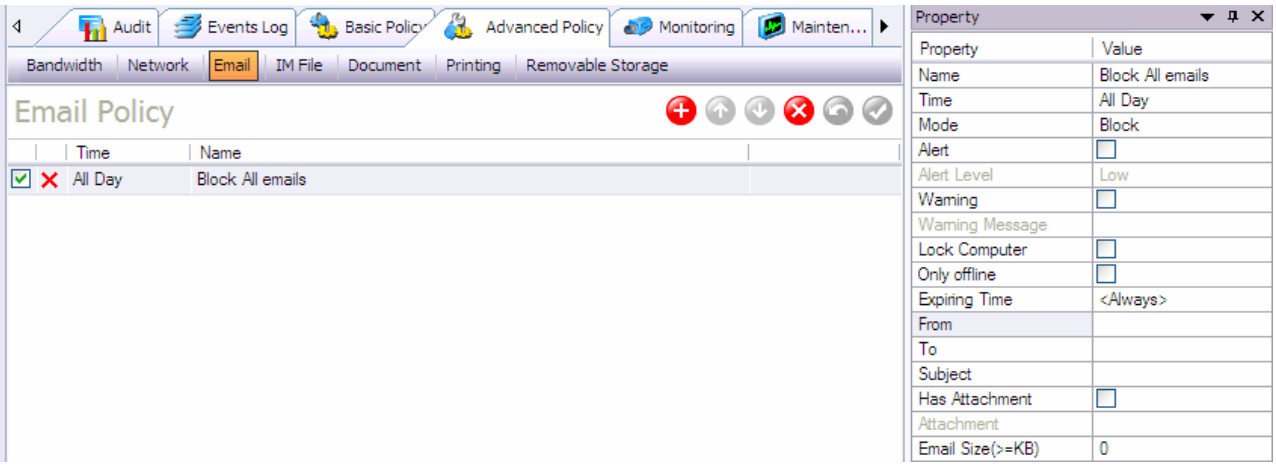


Figure 6.11 Mail Policy – Policy Example 1: 1st policy

Policy (2): Add another **Mail policy** to allow specified sender to send emails out.

Policy Name: **Allow @teclink.com.hk only**

Mode: **Allow**

Sender: ***teclink.com.hk***

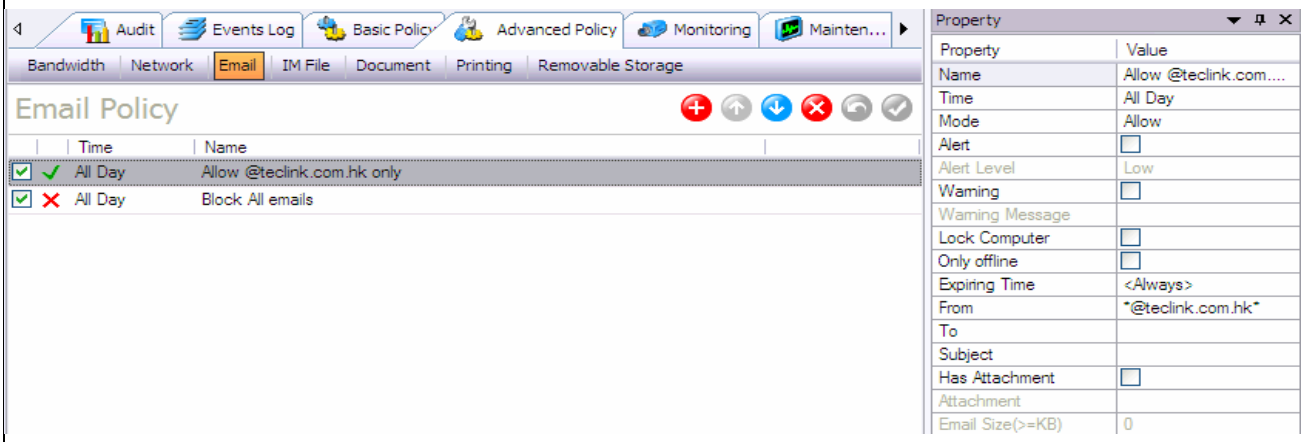


Figure 6.12 Mail Policy – Policy Example 1: 2nd policy

Mail Policy: Example 2

Requirements:

All Enterprises must not allow staff communicating with competitors, IP-guard can block all outgoing emails which the recipients are competitors

Policy (1): Add a **Mail policy** to block all emails which the recipients are competitors

Policy Name: **Block emails to send to competitors**

Mode: **Block**

Alert: **[optional]**

Warning: **[optional]**

Recipients: ***yahoo***

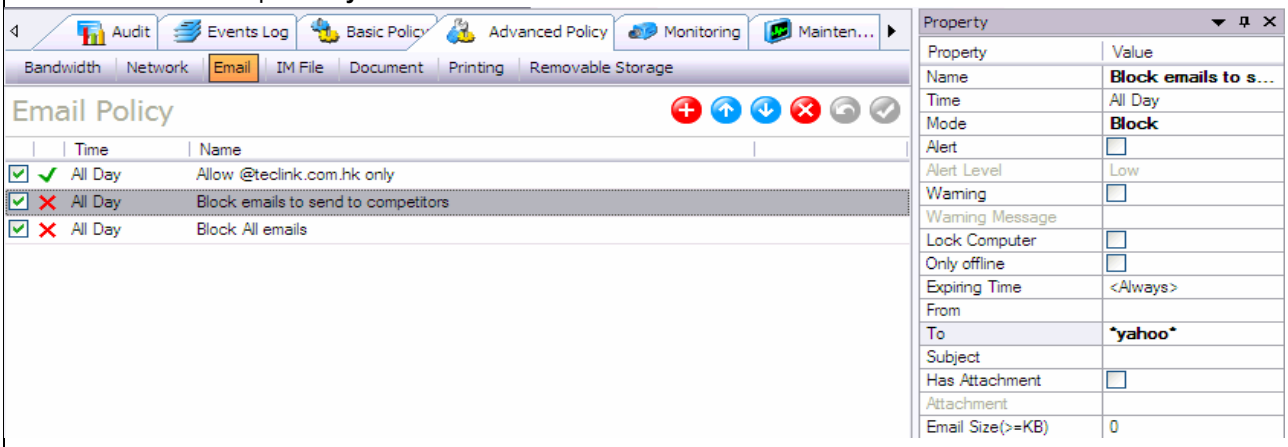


Figure 6.13 Mail Policy – Policy Example 2

6.13 IM File Policy

IM Policy is used to control the communications using IM tools and monitor/control all outgoing files sent through the IM tools to prevent information leakage through the IM channels

The following IM tools are supported to limit the outgoing files sent through IM tools: QQ, MSN, SKYPE, TM, UC, RTX, Yahoo!, POPO, ALI, ICQ etc.

Policy Properties:

File Name		Specify what files are controlled. Support wildcard input, using **;** or **,** as separators
Limited Size (>=KB)		Only enabled under the **block** mode. Used to limit the outgoing file size. Input range: 0 – 100000 (KB)
Backup		If checked, all outgoing files will be backup. The backup files can be retrieved from **Event log → Document**, check the option **has Backup** and select the operating type is **Upload/Send** for faster searching
	Minimum Size (>=KB)	If Backup is checked, the file size can specify to decide the file will be backup or not. If out of the specified range, the file will not be backup
	Maximum Size (<=KB)	

Table 6.12 IM Policy Properties

IM File Policy: Example 1

Requirements:

Some Enterprises may allow staff using IM tools for communications. However, they are also afraid that some information is sent out through these tools. Using IM policy to prohibit user to send files out and backup all trial outgoing files

Policy (1): Add an **IM File policy** to backup all outgoing files

Policy Name: **Backup all outgoing files**

Mode: **Allow**

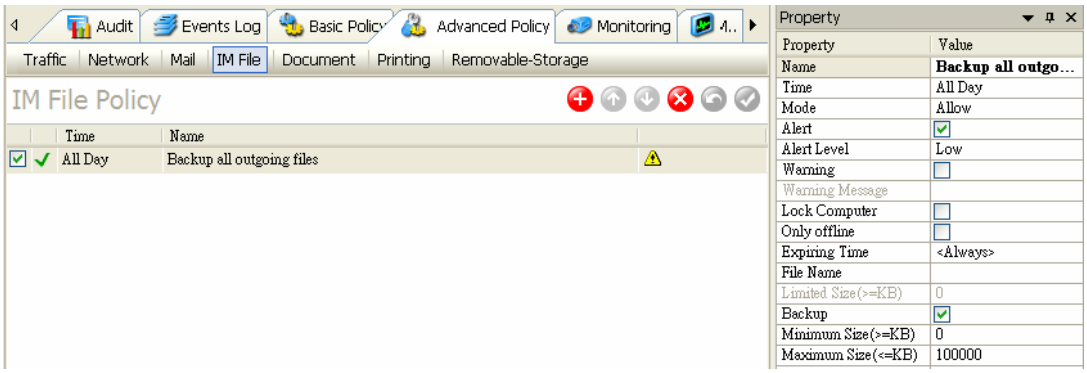


Figure 6.14 IM Policy – Policy Example 1: 1st Policy

Policy (2): Add another **IM File policy** to block all outgoing files with specified file extensions

Policy Name: **Backup all outgoing files with specified file extensions**

Mode: **Block**

Alert: **[optional]**

Warning: **[optional]**

File Name: ***doc*, *pdf*, *zip*, *rar*, *jpg***

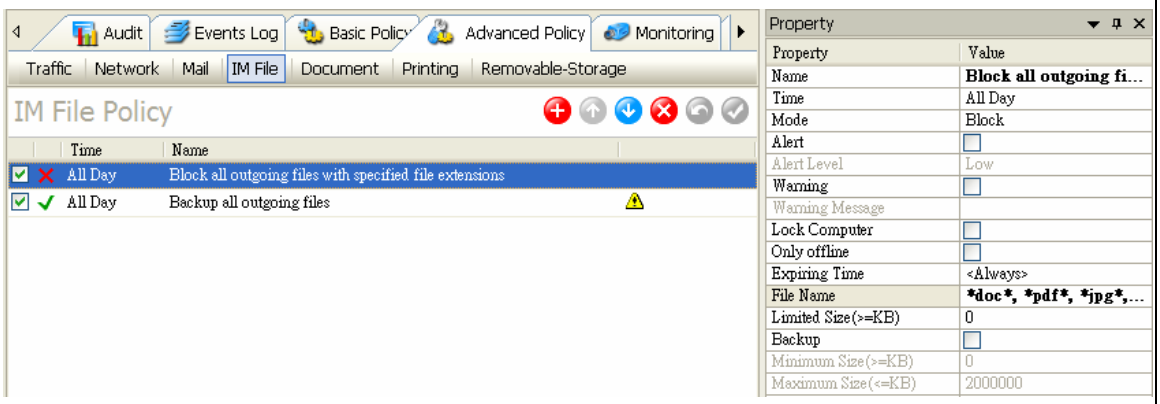


Figure 6.14 IM Policy – Policy Example 1: 2nd Policy

6.14 Document Operation Policy

Document Control Policy is used to control and limit the agent users accessing confidential information or assign different rights to different agent users. Also, the backup function prevents some important files are deleted maliciously or by human error

Policy Properties:

Operating Type		There are 3 kinds of operating types separated: Read, Modify and Delete - allow Modify means also allow to Read - allow Delete means also allow to Read and Modify
	Read	Read files
	Modify	Includes all operations expect read and delete, i.e. create, rename, modify, copy, move and restore.
	Delete	Delete files
Disk Type		By default, it is set to <All>, Press Ctrl + A to select all or none.
File Name		- Specify the required control filename, also can input the folder path e.g. E:\work*, it represents all files under this work folder take effective of that particular policy. - Support wildcard input, using ; and , as separators for multiple inputs
Backup before modify		- Backup files before modify - This option is only enabled when **Modify** is checked
Backup when copy/out to		- Backup files when copy/cut to specified disk - This option is only enabled when **Modify** is checked
Backup when copy/out from		- Backup files when copy/cut from specified disk - This option is only enabled when **Modify** is checked
Backup before delete		- This option is only enabled when **Delete** is checked
Minimum Size (>=KB)		If the above Backup options are checked, the file size can specify to decide the file will be backup or not. If out of the specified range, the file will not be backup
Maximum Size (<=KB)		
Application		Specify the document operations done on application software

Table 6.12 Document Policy Properties

Document Operation Policy: Example 1

Requirements:

Some important files/folders from shared network drive are required to restrict not all users can modify or delete the files

Policy Settings:

Policy (1): Add a **Document Control policy** to block the operating types: modify / delete to specified network shared drive

Policy Name: **Cannot modify / delete \\network_path***

Mode: **Block**

Alert: **[optional]**

Warning: **[optional]**

Operating types: **check modify, delete**

Disk type: **Network**

File Name: **\\network_path***

Property

Property	Value
Name	only can access \\192.168....
Time	All Day
Mode	Block
Alert	☑
Alert Level	Critical
Warning	☑
Warning Message	You are not allowed to mo...
Lock Computer	☐
Only offline	☐
Expiring Time	<Always>
Operating Type	Modify Delete
Read	☐
Modify	☑
Delete	☑

Disk Type	Network
File Name	\\192.168.0.156*
Backup before modify	☐
Backup when copy/cut to	☐
Backup when copy/cut from	☐
Backup before delete	☐
Minimum Size(>=KB)	0
Maximum Size(<=KB)	100000
Application	<All>

Figure 6.15 Document Policy – Policy Example 1

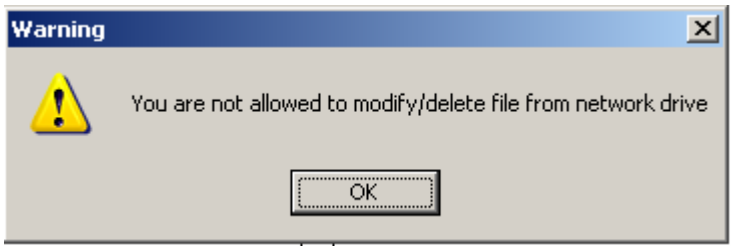


Figure 6.16 Document Policy – Policy Example 1 Warning message

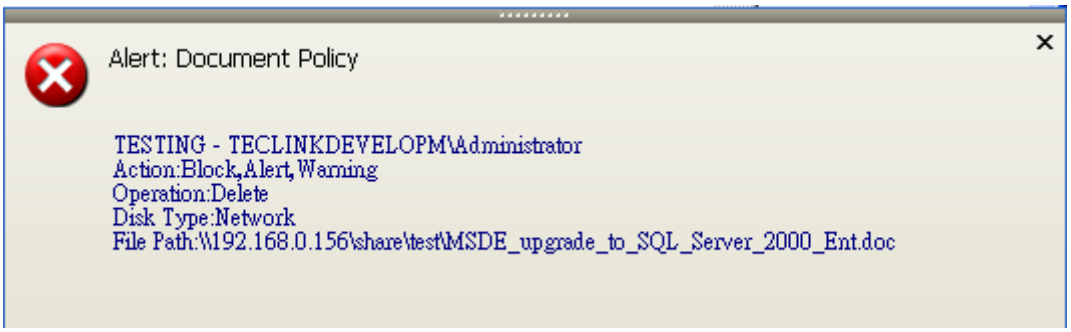


Figure 6.17 Document Policy – Policy Example 1 Alert message

Document Operation Policy: Example 2

Requirements:

Similar to the Example Policy 1, however, to facilitate the network shared resources, some staff is allowed to modify/delete files/folders from shared network drive but System administrator is afraid that some files are deleted maliciously or by human error. In this case, backup options should be checked in a document control policy.

Policy Settings:

Policy (1): Add a **Document Control policy** to allow the operating types: modify / delete to specified network shared drive

Policy Name: **Backup files before delete**

Mode: **Allow**

Alert: **[optional]**

Warning: **[optional]**

Operating types: **check modify, delete**

Disk type: **Network**

File Name: **\\network_path***

Backup before delete: **checked.**

All backup files can be retrieved from **Event Logs → Document**

Figure 6.18 Document Policy – Policy Example 2 Document Operation Logs

Caution:

Be careful of Backup Option

If any Backup options are checked, it will cause the volume of backup data quite large. We strongly recommend the System administrator should be careful when designing their policies with backup options. Enough hard disk spaces should be ready for storing the data and keep to backup the data regularly.

6.15 Printing Policy

Printing policy is used to control the use of different kinds of printers such as local, shared, network and virtual printers to prevent the information leakage.

Policy Properties:

Printer Type	4 kinds of printer types: Local, Shared, Network and Virtual Printer (e.g. PDF creator)
Printer description	Set the printer name. System administrator can specify the internal network printers e.g. \\server* represents all printers in \\server
Application	Specify the application used for printing out
Record Printed Image	Record the printed out document

Table 6.13 Printing Policy Properties

Printing Policy: Example 1

Requirements:

Some Enterprises are afraid that their staff brings their own mini-printers back to office to print out confidential information/data

Policy Settings:

Policy (1): Add a **Printing policy** to block all local printers

Policy Name: **Block all local printers**

Mode: **Block**

Printer Type: **Local Printer**

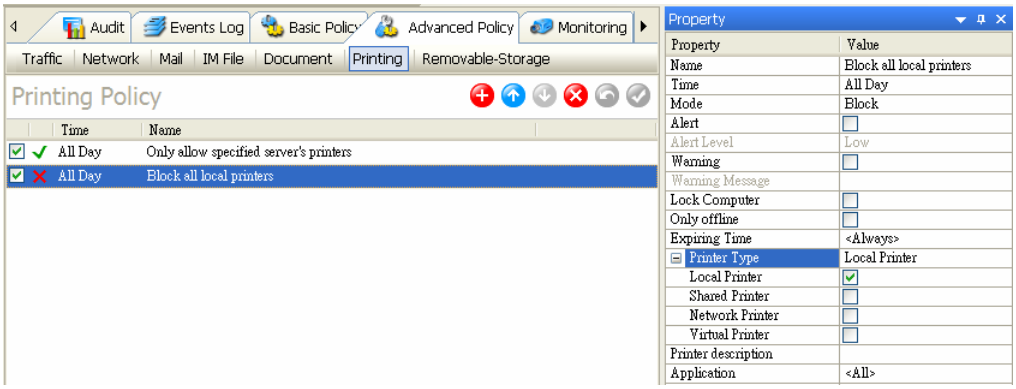


Figure 6.19 Printing Policy – Policy Example 1: 1st Policy

Policy (2): Add another **Printing policy** to allow specified server's printers

Policy Name: **Allow specified server's printers**

Mode: **Allow**

Printer Type: **Shared Printer, Network Printer**

Printer description: **\\192.168.0.72***

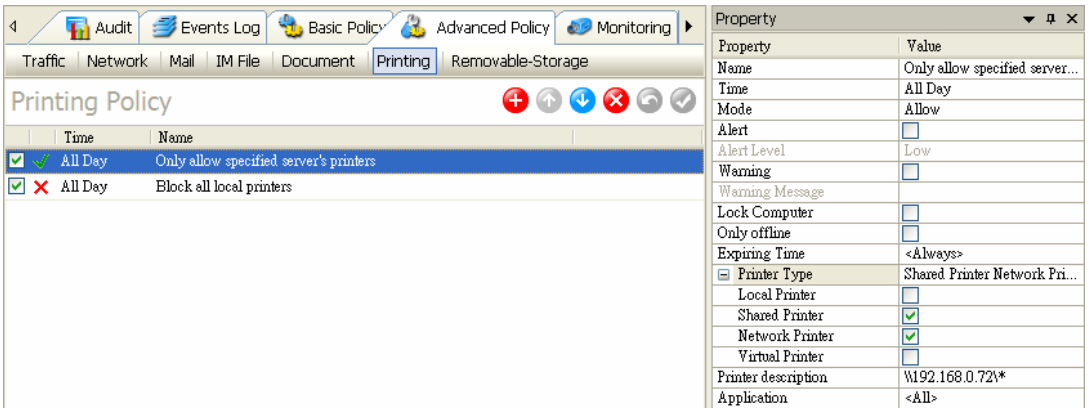


Figure 6.20 Printing Policy – Policy Example 1: 2nd Policy

6.16 Removable-Storage Policy

To prevent information leakage through removable devices, System administrator can apply removable-storage policy to assign different rights to removable storages. Also, the files can be encrypted when writing to the removable storages, only authorized computer agents can decrypt the files.

To manage specified removable storages, go to **Tools → Classes Management → Removable-Storage** or refer to Section 12.4.3 to see how to custom the Removable-storage classes

Policy Properties:

Read	- free to read any files from removable storages - The following 3 options (i.e. **Decrypt when reading**, **Write** and **Encrypt when writing**) are enabled when this is checked
Decrypt when reading	- this option is only enabled when **Read** is checked - the files are only decrypted using Explorer.exe to copy files from removable storage to local or network disks. Using other application programs to read the encrypted files cannot be decrypted
Write	- free to write any files to removable storages - when the action **Write** is prohibited, any files cannot be copied or saved to removable storages, also, all files in the removable storages cannot be deleted or renamed.
Encrypt when writing	- this option is only enabled when **Write** is checked - Prohibit any application programs to copy any files to removable storages except using Explorer.exe
Removable Storage	By default, it is set to <All>.To specify removable storages, corresponding classes must be selected (Please refer to Section 12.4.3 about Removable-storage class management)

Table 6.14 Removable-storage Policy Properties

Removable-storage Policy: Example 1

Requirements:

How to control users that only can use company's provided removable devices?

Policy Settings:

Policy (1): Add a **Removable Storage policy** to block all unclassified devices

Policy Name: **Block all unclassified devices**

Read: **unchecked**

Removable Storage: select **{Unclassified}** class

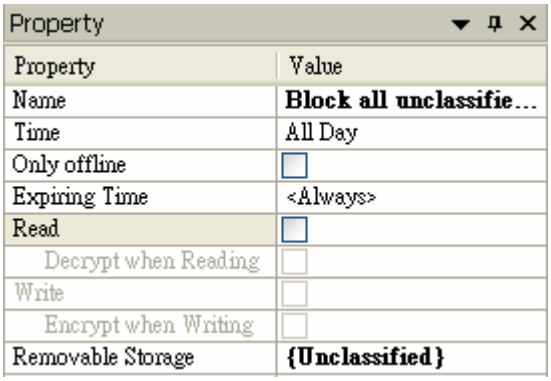


Figure 6.21 Removable-storage Policy – Policy Example 1: 1st Policy

Policy (2): Add another **Removable Storage policy** to allow approved class removable-devices

Policy Name: **Allow Read/Write for approved class device only**

Read: **checked**

Write: **checked**

Removable Storage: select **{approved}** class

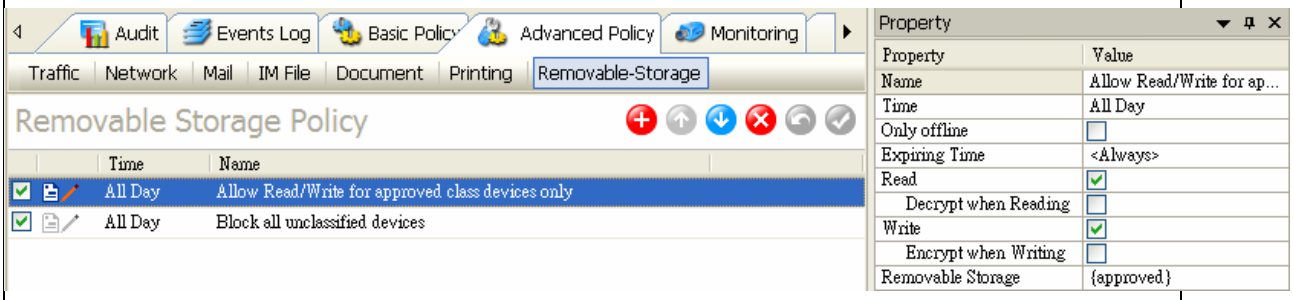


Figure 6.22 Removable-storage Policy – Policy Example 1: 2nd Policy

Caution:

Priority between Document Control Policy and Removable-storage Policy

If both document control policy and removable-storage policy are applied at the same time, document control policy will be executed first and then removable-storage policy. For instance, in removable-storage policy, a policy allows reading/writing from removable storage with encrypt function; while in document control policy, a policy prohibits all word document to copy to removable disk. The resulting execution is not allowed copying any word documents to removable disk but other files are allowed copying to removable storage with encryption.

Chapter 7 Monitoring

7.1 Instant Message Monitoring

System administrators are able to monitor Instant Message history of Agent computers by selecting **Monitoring→Instant Message**. Supported instant message tools include: Tencent QQ, TM, MSN Messenger, ICQ (Not support web-based ICQ yet), Yahoo! Messenger, Sina UC, 163 POPO (outgoing message only), Skype (support both since v3.0.2108), Tencent RTX, Lotus Sametime, and Alibaba AtiTalk.

Figure7.1 Instant Message

The Instant Message log includes: IM tools, Computer, Local user, Contact User, Begin Time, End Time, no. of Statement and the Instant Message contents

IM Tool	Show which IM tool is used
Computer	Show the computer name
Local User	Show the IM login account
Contact User	Show the another chatting party's user account
Begin Time	Show the start time of chat
End Time	Show the end time of chat
Statement	Show the total numbers of chat statement
IM Content	Show the details of IM contents with recorded time

Table 7.1 IM Log Contents

Save IM Contents

To save the IM contents, select the desired records (press Ctrl for multiple selections) and then right click to select **Save As HTML File** to save the IM contents in **htm** or **html** format. If multiple records are selected, each one will be saved in individual file.

Search conditions

Tool	By default, it is set to **All**. To specify IM tool can select from the drop down menu
User ID or Nickname	Query the IM contents with specified either local user ID (or nickname) or another party's account ID (or nickname)
Content	Query the IM contents with specified the keywords input e.g. *mail* The input contents will be highlight with red color in the results

Table 7.2 IM Search Conditions

7.2 Email Monitoring

Email contents can be logged from every agent. Support email types: Normal mail, Exchange mail, Web mail and Lotus mail. Note that only normal and Exchange mail types can log all incoming and outgoing emails, web mail and Lotus mail types can only log the outgoing mail.

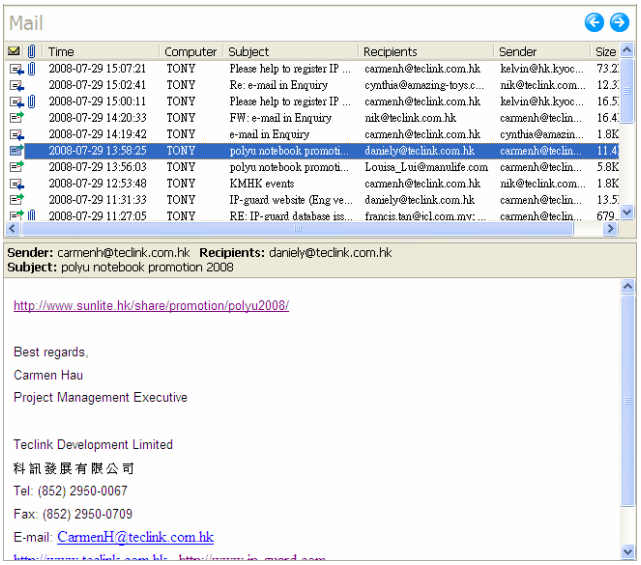


Figure 7.2 Mail Monitoring

Email contents include: Send/Receive, Subject, Sender, Recipients, mail content, attachment and size.

Send/Receive	represents the mail is outgoing email while represents the mail is incoming email
Subject	Subject of email
Sender	Sender's email address
Recipient	Recipients' email address including CC and BCC email address, the details can be reviewed in the property windows
Attachment	represents the mail has attachment. By default, system will backup all email attachments (System administrator can add a Logging policy to not backup the attachment, details please refer to Section 6.7). Click button to retrieve the attachments.
Size	Email size
Content	Select one of the email first, the details will be showed at the bottom part.

Table 7.3 Mail Log Contents

Save emails

To save the email contents, select the desired records (press Ctrl for multiple selections) and then right click to select **Save As EML File** to save the email contents in **eml** format. If multiple records are selected, each one will be saved in individual file.

Search Conditions

Type	By default, it is set to All. To specify email type can select from the drop down menu
Send/Receive	By default, it is set to All. Or either query send or receive only
Email address	Query specified email address
Subject	Query email with specified keywords input about the email subject
Content	Query the email contents with specified the keywords input e.g. *mail* The input contents will be highlight with red color in the results
Attachment	If this option is checked, all email with/without attachment will be queried. If this option is not checked, only email with attachment will be queried.
Attachment name:	Query email with specified keywords input about the attachment
Size	Query email with specified email size range

Table 7.4 Mail Search Conditions

7.3 Real-time Screen Snapshot

System administrator can monitor and track the screen snapshot of a computer/user by selecting **Monitoring→Screen Snapshot.**

	If a computer is logged by two or more users or same user logged into two or more computers, manager can select which screen to display by clicking this button.
	Best fit windows size.
	Original windows size.
	Track button, the screen snapshot is automatically refreshed. The refresh interval setting can be set in **Tools→Options→Console Settings→Information→Interval of tracing frames (seconds)**
	Stop Track, the screen snapshot will not be refreshed.

Table 7.5 Screen Snapshot Functional Buttons

Figure 7.3 Screen Snapshot Monitoring

After selecting a target computer, click the **Track** button to start the real-time tracking function. Then, the screen snapshot will update when the target computer's screen is changed. The track mode could be stopped by clicking the **Track** button again.

7.4 Multi-Screen Monitoring

System administrator could monitor the screen snapshot of multiple target computers. Multi-Screen monitoring display is a screen matrix and the matrix size is from (2 x 2) to (4 x 4). This function could be started from menu **Monitoring →Multi-Screen**.

System will update the screen snapshot periodically with specified matrix size. Next matrix of computers will be updated after a period of time.

Functional Buttons

	First page of screen matrix
	Previous page of screen matrix
	Next page of screen matrix
	Last page of screen matrix
	Full screen mode to display one or multiple screen snapshots. Double click one of the screen snapshot to view it individually. Press **ESC** on the keyboard to resume to windows mode.
	Specify the required monitored computer or computer group
	Close to exit the Multi-screen viewer

Table 7.6 Screen Snapshot Viewer Functional Buttons

Lock Function

You could lock on one of the screen of a computer by using the lock on function. Right click on the target computer screen snapshot, and then select **Lock**. When the screen is locked, the background of the title of that screen snapshot will change to yellow. Once the screen is locked, it will stay right here even the screen switch to next group after a period of time. If you want to release the screen, click the **Lock** button again to release the screen.

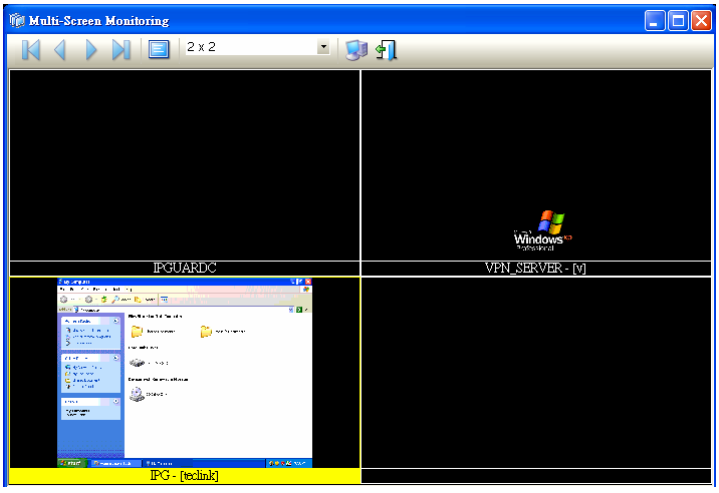


Figure 7.4 Multiple Screen Monitoring

Screen Snapshot information

When mouse moves to one of the snapshot, it will display the agent information including Computer name, IP address, User and online status.

Refresh Interval Setting

The update period of the screen snapshot could be configured in **Tools→Options→Console Settings→Information→Interval of tracing frames (seconds)**

7.5 Query Screen Snapshot History

Select **Tools→Search Screen History** to search the screen snapshot history

Search conditions

Begin / End Date	Query the screen snapshot history with specified begin and end date
Name	Query the screen snapshot history with computer name. Support wildcard input e.g. **TEC**. Then the resulting query will only include all screen snapshot history with computer name TEC
IP address	Query the screen snapshot history with specified IP address. Either input a IP address or a IP address range e.g. 192.168.1.100-192.168.1.200

Table 7.7 Screen Snapshot Search Conditions

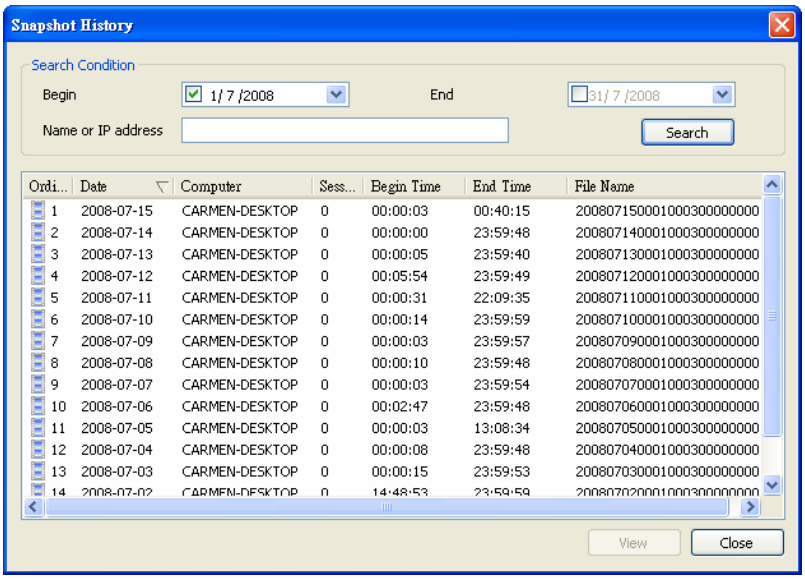


Figure 7.5 Snapshot History

History Log Properties

The log information include: Date, Computer, Session, Begin Time, End Time and File Name

Date	The recording date of the screen snapshot history. Basic unit is “Day”, a file is used to store one day snapshot history
Computer	Computer name for corresponding screen snapshot history
Session	If only one user logon, the session ID is 0. The second logon user, the session ID is 1. Every session ID would have its own file to store the snapshot history Notes that the first user logon session ID is 1 under Windows Vista
Begin / End Time	The start and end time of snapshot history
File Name	The file name shows as <SQL>, it represents that the screen snapshot data is stored inside the SQL server. If the screen snapshot files are stored under the SCREEN directory, the file name is initialized at date

Table 7.8 Screen Snapshot History Log Properties

7.6 View Screen Snapshot History

Double click one of the resulting records or click **View** button after a record selected. The Screen History Viewer will open. Notes that the viewer cannot run individually, it must be run during IP-guard console is running

7.6.1 Screen Snapshot Viewer

In the Screen Snapshot Viewer, it includes: the menu bar, tool bar, searching bar, time line bar, display panel, as well as the status bar.

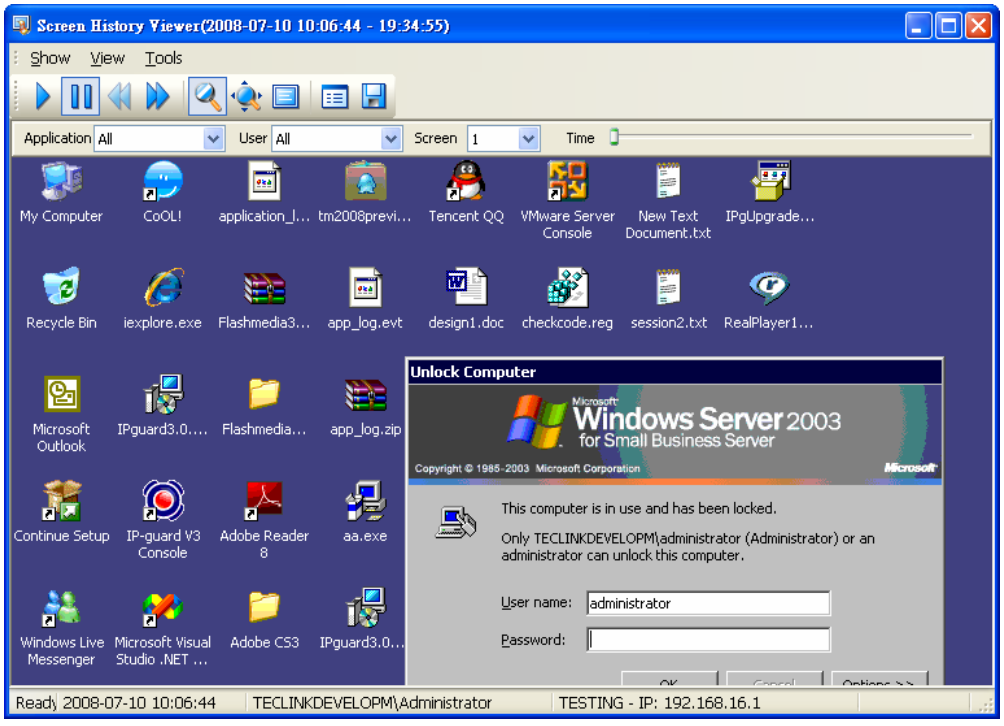


Figure 7.6 Screen Snapshot History Viewer

7.6.2 Display

Select **Show → Play** to start to play the screen snapshot history

	Play the screen snapshot history continuously
	Stop
	Display the Previous capture
	Display the Next capture

Table 7.9 Screen Snapshot History Viewer Functional Buttons

Except using the control buttons, System administrator can also control the time line bar to point to the specified capture directly.

7.6.3 View Menu

From the menu bar, the view menu includes **Toolbar**, **Status bar**, **Original Size**, **Fit to Window**, **Full screen** and **Play Speed**. System administrator can select their desired options to meet their needs such as fitting the windows size or display in full screen mode. Also, there are 3 options in **Play Speed**: Slow, Normal and Fast. It can be adjusted for playing the screen snapshot history.

7.6.4 Search Bar

According to the specified **Application**, **User**, **Screen** and **Time line** to display the matched screen snapshot history

Application	By default, it is set to All. To specify viewed application can select from the drop down menu. Once selected, only the specified application snapshot will be showed.
User	By default, it is set to All. To specify the user can select from the drop down menu. Once selected, only the specified user snapshot will be showed.
Screen	If agent side has more than one display card installed or a display card with multiple connected interfaces, one of them can be specified to play.
Time line	Display the current time frame, drag the slider to a designated location to view the current frame of the screen. When mouse is over the time line pointer, the basic information: **Time**, **User**, **Application** and **Caption** will appear

Table 7.10 Screen Snapshot History Viewer Functional Buttons

7.6.5 Export

Select from **Tools→Save as Video Files…** to save the screen snapshot history in **wmv** format. There are 4 options provided before saved.

From / To Time	Drag the slider to designated from and to time, only the specified time range record will be exported
Application	If this is checked, the default is set to All. To specify the Application can select from the drop down menu. Once selected, only the specified Application record will be exported
User	If this is checked, the default is set to All. To specify the User can select from the drop down menu. Once selected, only the specified User record will be exported
All	If this is checked, all screen snapshot history will be exported

Table 7.11 Screen Snapshot Export Function

Chapter 8 Remote Maintenance

According to the research analysis, many internal IT department staff (esp. technical support staff) may spend 70-80% time on daily maintenance tasks. The functions of Remote Maintenance in IP-guard help IT department real-time check the computers' status and information. With real-time information helping to solve the technical problems immediately to save more time and resources especially in assisting remote sites' computers.

8.1 Remote Maintenance

8.1.1 Applications

Select **Maintenance→Applications** can check the agent running application status. The active running application is highlighted in blue color.

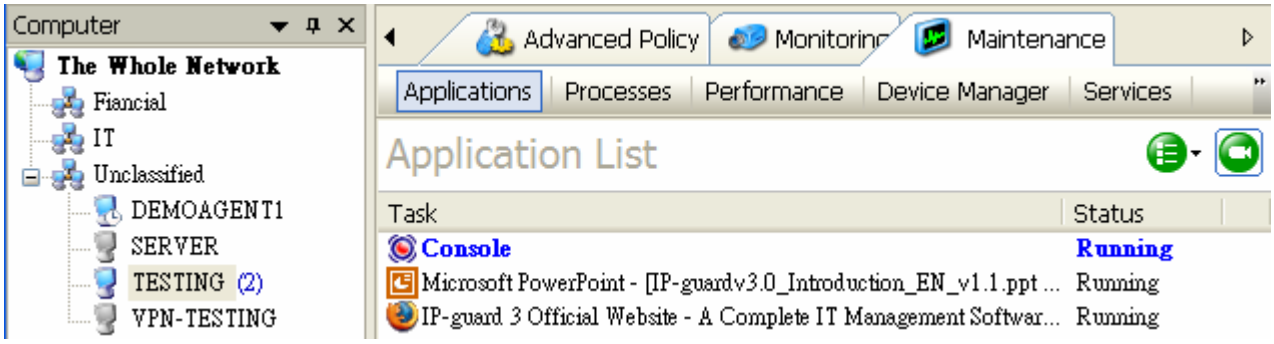


Figure 8.1 Remote Maintenance – Applications

Control Buttons:	
	For the terminal server situation, there are some concurrent connections and different users logon at the same time, click this button can select specified user to check their application running status.
	This is trace button, click this button the application list will be refreshed automatically. The refresh time interval set from **Tools→Options→Console Settings→Information→Maintenance**
Remote Controls:	
End Task	Select any application from Application List, right click and select **End Task** to stop the running application program

Table 8.1 Application List Controls

8.1.2 Processes

Select **Maintenance→Processes** can check the agent's all real-time processes including: Filename, PID, time, CPU, CPU Time, Memory, Virtual Memory, Priority, Handle, Thread Count and Path.

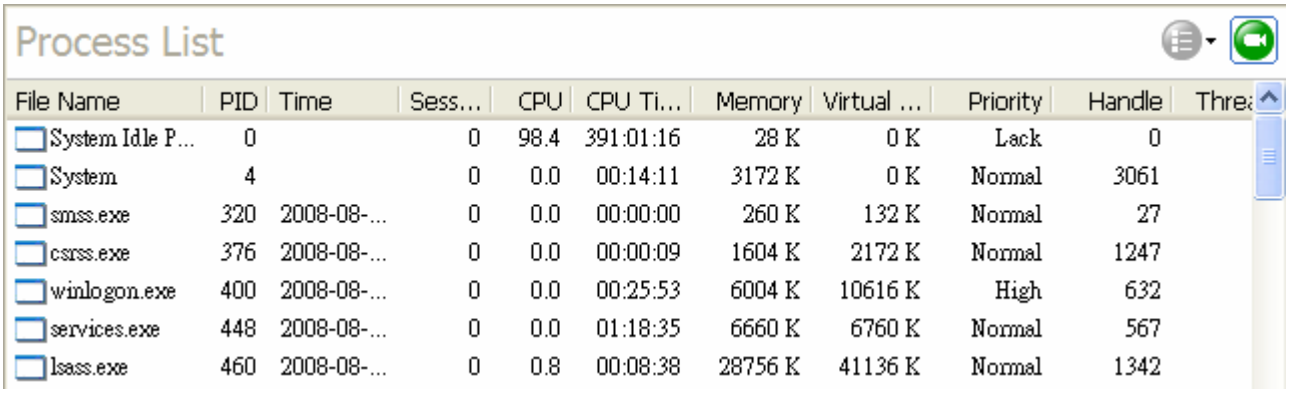


Figure 8.2 Remote Maintenance - Process

Time	Startup time of the process
Path	Details path of the process
Other	Other properties are like the processes running in Explorer.exe, their meanings are similar

Table 8.2 Process List Contents

Control Buttons:	
	Only enable under user mode (see Figure 8.3), select target user to check the processes status.
	This is trace button, click this button the processes list will be refreshed automatically. The refresh time interval set from **Tools→Options→Console Settings→Information→Maintenance**
Remote Control:	
End Task	Select any processes from Processes List, right click and select **End Task** to stop the process

Table 8.3 Process List Controls

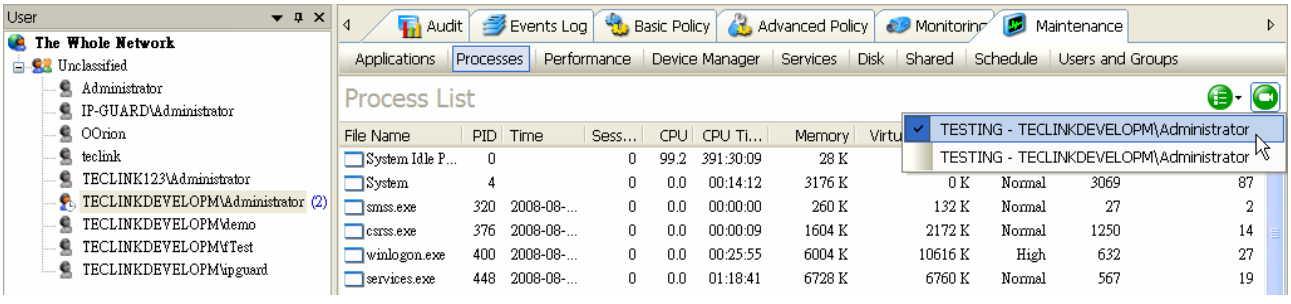


Figure 8.3 Remote Maintenance – Checking Process for multiple logon users

8.1.3 Performance

Select Maintenance→Performance can check the agent's performance status including CPU Usage, Memory Usage, Physical Memory, Commit and Kernel Memory. These real-time data is exactly same as **Windows Task Manager → Performance**

Control Buttons:

	Only enable under user mode, select target user to check the performance status.
	This is trace button, click this button the processes list will be refreshed automatically. The refresh time interval set from **Tools→Options→Console Settings→Information→Maintenance**

Table 8.3 Performance Controls

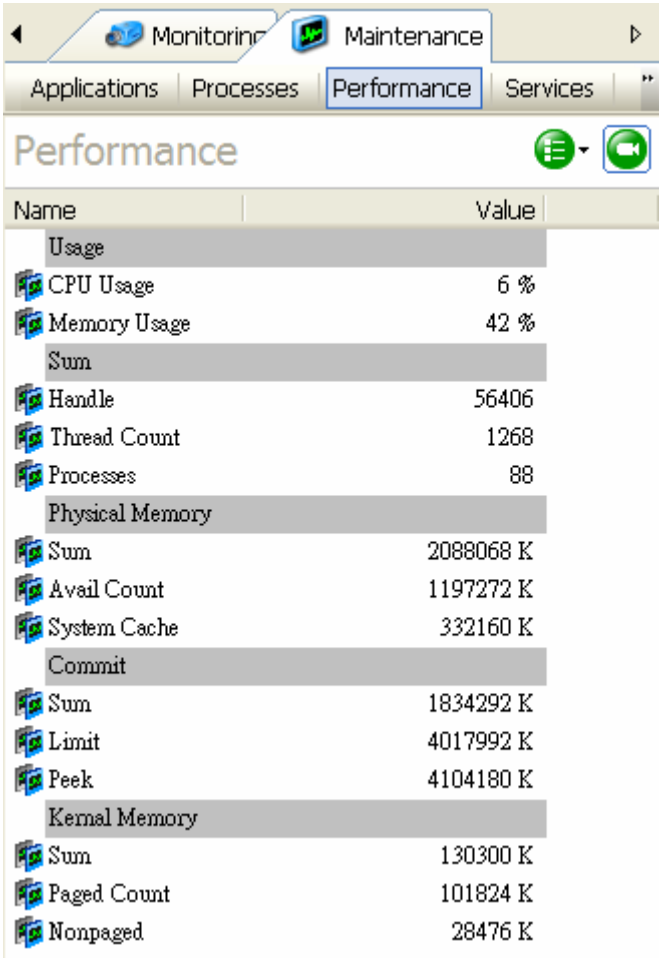


Figure 8.4 Remote Maintenance – Performance

8.1.4 Device Manager

Select **Maintenance→Device Manager** to check the agents' all devices including Processor, DVD/CD ROM Drive, Keyboard, Mouse, Network adapters etc.

Control Buttons	
	Device List Checking method: **By Type**, **By Connection** and **Show Hidden Devices**
	Only enable under user mode, select target user to check the device.
Remote Controls:	
Disable / Enable	Select target device, right click to select **Disable** or **Enable** to control agent's devices

Table 8.4 Device Manager Controls

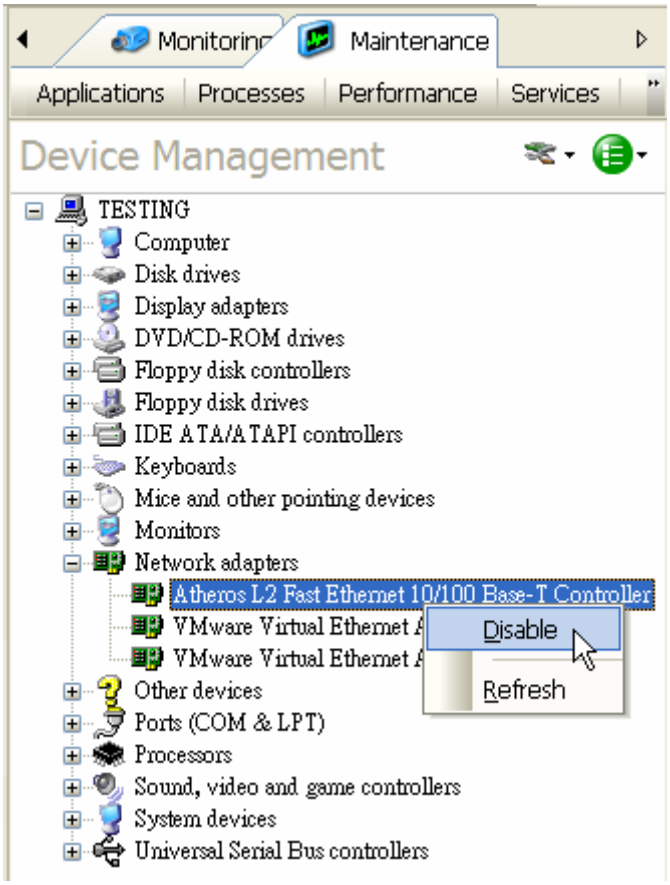


Figure 8.5 Remote Maintenance - Device Manager

8.1.5 Services

Select **Maintenance→Service** to check the agents' system services information including Name, Description, Status, Startup Type, Log On As and Path.

Control Buttons:	
	Only enable under user mode, select target user to check the device.
Remote Control:	
Start / Stop	Select target service, right click to select **Start** or **Stop** to control system service
Startup Type	Select target service, right click to select Startup Type. There are three types can be set: Automatic, Manual and Disabled

Table 8.5 Service Controls

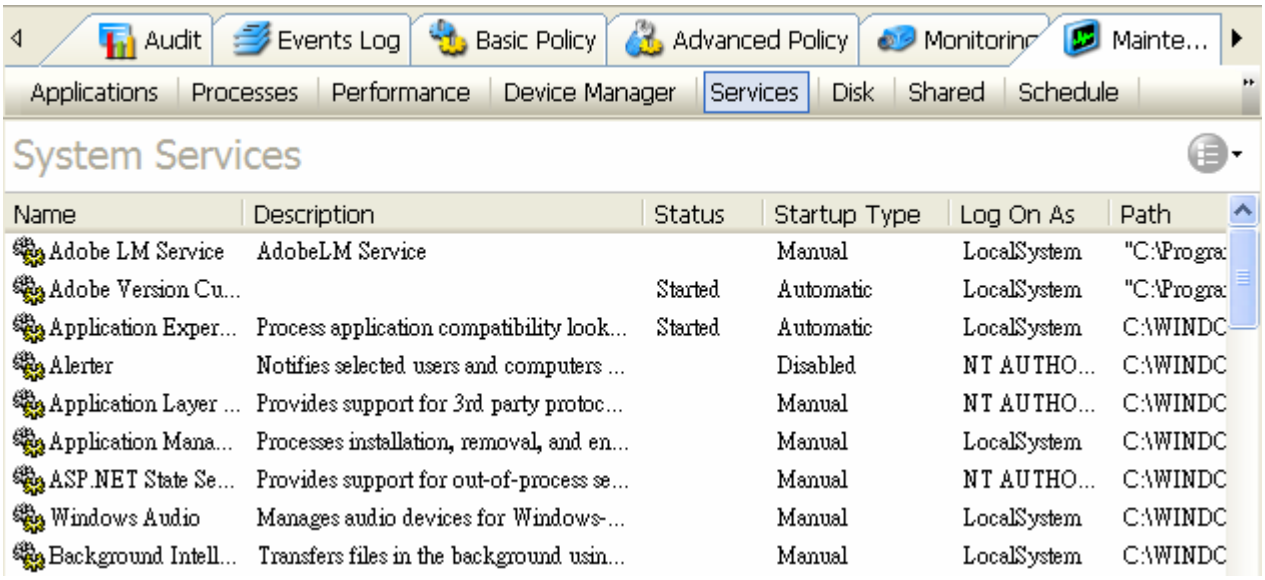


Figure 8.6 Remote Maintenance – System Services

8.1.6 Disk

Select Maintenance→Disk can check the agent's disk usage situation including disk Volume, File System, Capacity, Free Space and % Usage

Control Buttons:

	Only enable under user mode, select target user to check the disk information.

Table 8.6 Disk Controls

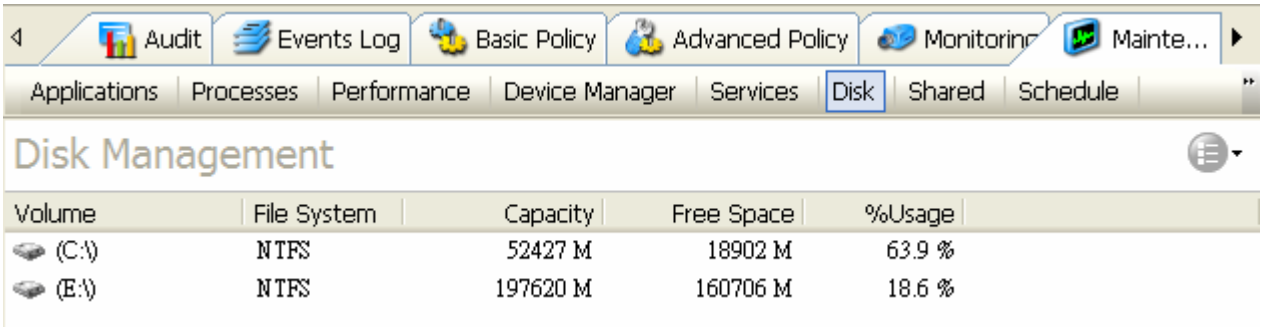


Figure 8.7 Remote Maintenance – Disk

8.1.7 Shared

Select **Maintenance→Shared** to check the agents' network shared situation including shared folders, shared Path, Client Connections and Comments.

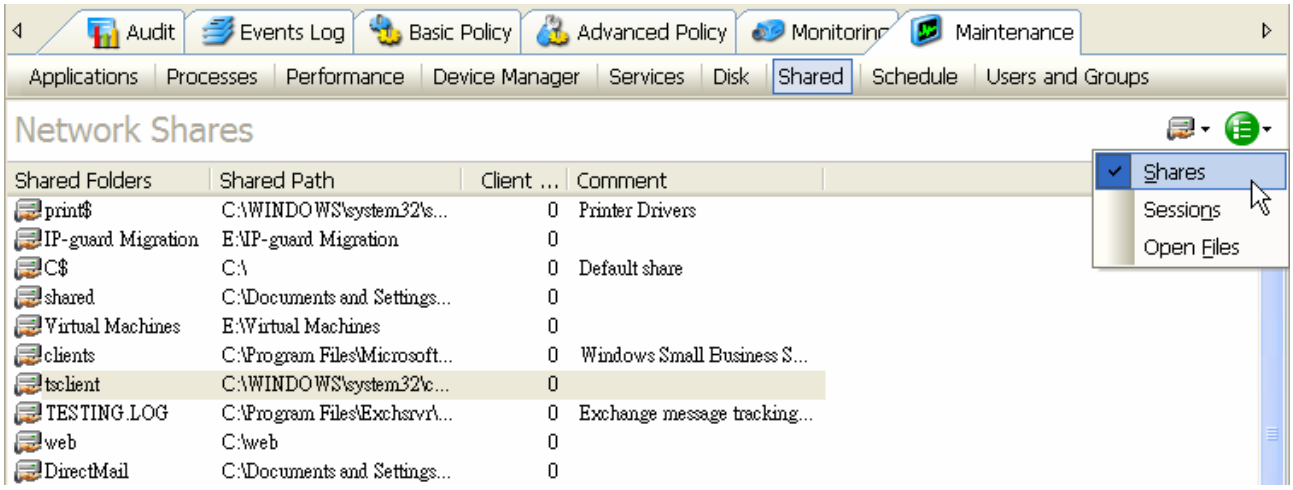


Figure 8.8 Remote Maintenance – Network Shares

Control Buttons:	
	Only enable under user mode, select target user to check the network shares status.
Remote Control:	
Share	Select target network share, right click to select **Delete share** to delete the shared
Sessions	Select this mode to check agent's shared files is being remote accessed by remote computers or not. The information includes User, Computer, Type, Open File, Connect Time, Idle Time and Guest (see Figure 8.7)
Files	Select this mode to check the files operation details which are being remote accessed including Open File, Visitor, Locked and mode. System administrator can select target file, right click to select **Close Open File** or **Close All Open Files**

Table 8.7 Shared Controls

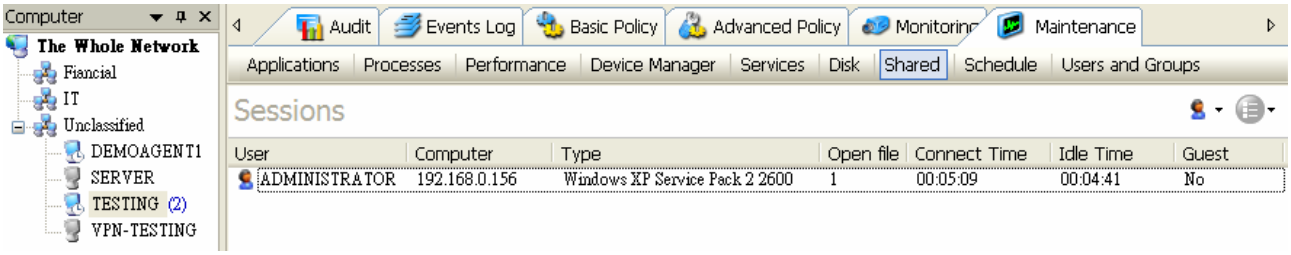


Figure 8.7 Remote Maintenance – Network Shares (Sessions Mode)

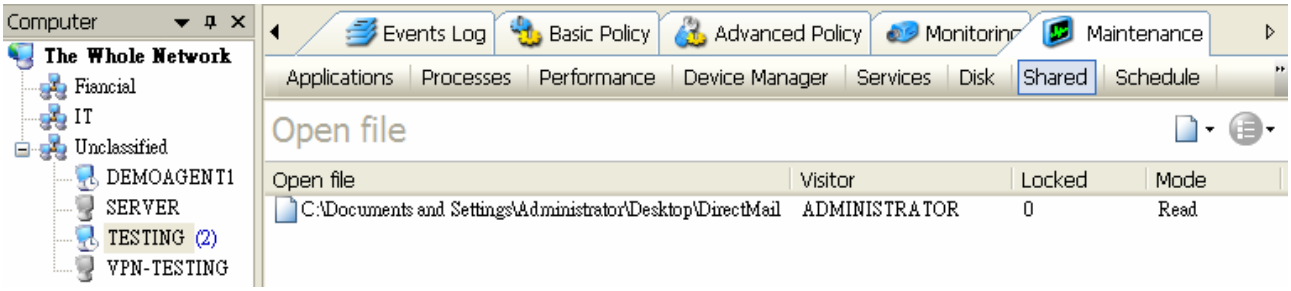


Figure 8.8 Remote Maintenance – Network Shares (Open File Mode)

8.1.8 Schedule

Select **Maintenance→Schedule** can check the agents' computers schedule list including Name, Schedule, Application, Next Run Time, Last Run Time, Status, Last Result and Creator

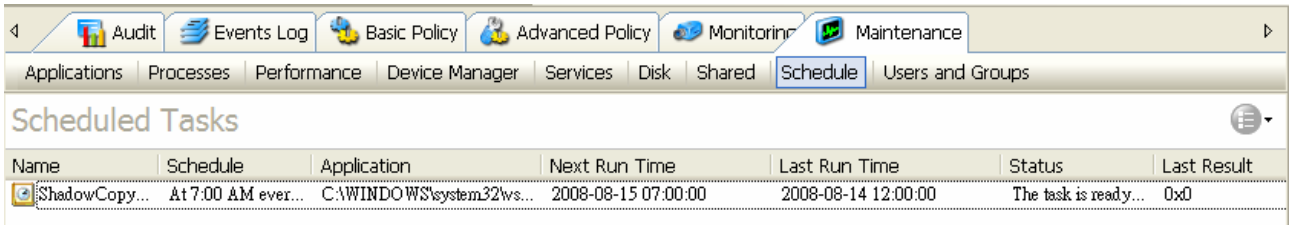


Figure 8.9 Remote Maintenance – Schedule

Select the schedule task, right click to select **Delete** to delete the schedule.

Control Buttons:

	Only enable under user mode, select target user to check the schedule status.

Table 8.8 Schedule Controls

8.1.9 Users and Groups

Select **Maintenance→Users and Groups** to check the agents' computer all local users and groups. The information for local users includes Name, Full Name and Description while for groups includes Name and Description.

Control Buttons:

	Only enable under user mode, select target user to check the users and groups information.

Table 8.9 User and Groups Controls

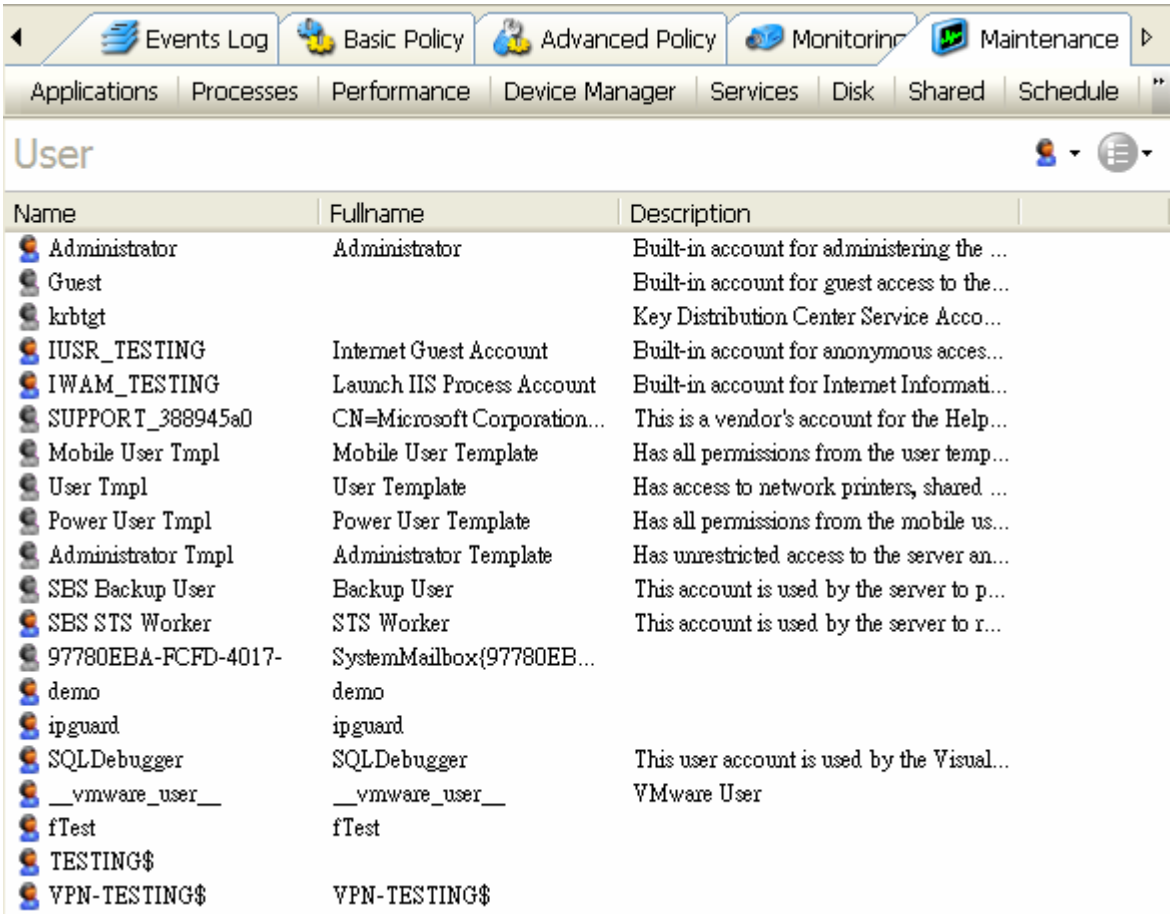


Figure 8.10 Remote Maintenance – Users and Groups

8.2 Remote Control

8.2.1 Remote Control

Select target agent computer from the network tree, then select **Maintenance→Remote Control** or right click to select **Control→Remote Control**. There are 2 types of authorization methods for remote control: agent user authorization and password authorization

Agent User Authorization

Select target computer, select **Maintenance→Remote Control** or right click to select **Control→Remote Control**, a popup windows from Console requests authorization from agent side (see Figure 8.11), click **Yes**. Then a popup window appears in agent computer to ask for authorization from remote side (see Figure 8.12). If the agent user answers Yes, System administrator can control the agent computer immediately from the Console.

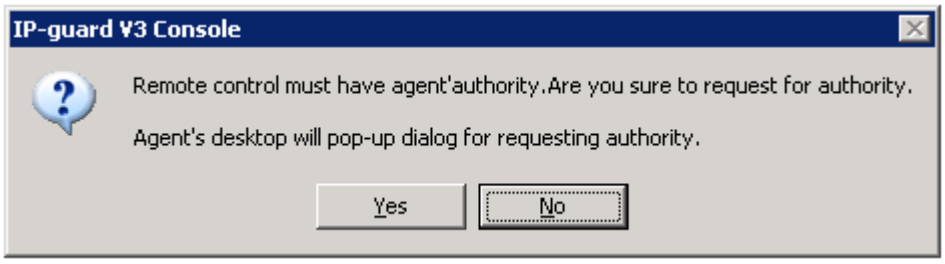


Figure 8.11 Console requests authorization from agent side

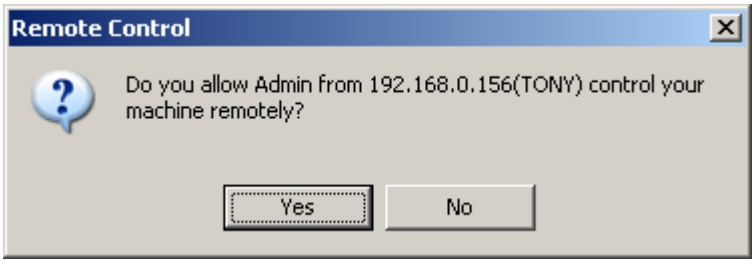


Figure 8.12 Ask for authorization from remote request

Password Authorization

Select target computer, select **Maintenance→Remote Control** or right click to select **Control→Remote Control**, a popup window (see Figure 8.13) appears in the Console to request to input the password. If the password is correct, System administrator can control the agent computer immediately. Otherwise, the control is ended.

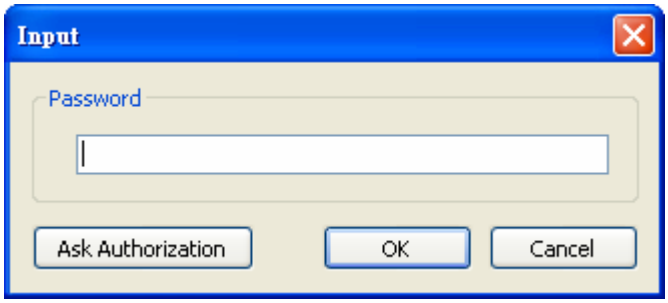


Figure 8.13 Input password for remote control

The method to preset the password from agent computer is: Press **ctrl + alt + shift + ocularrm** from the keyboard, then a popup window (see Figure 8.14) would appear in the agent computer, input the password twice to confirm.

Figure 8.14 Set remote password in agent computer

To protect the agent users against the preset password method, System administrator can set a policy in Remote Control Policy to force all authorizations must be granted from agent users even the agent computer has set the password (Details please refer to Section 6.8 Remote Control Policy)

Remote Control Interface

When the agent computer is in remote control status, a message **Remote Controlling…** would display at the right upper corner to inform the agent user that his/her computer is under remote control.

Functional Buttons:

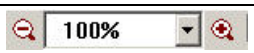
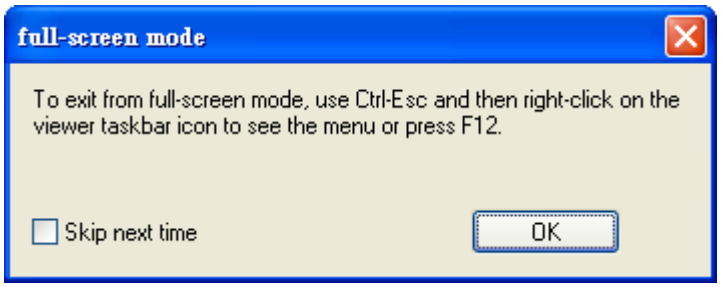
	Screen Size
	Full screen mode. To exit from full-screen mode, press **F12 or** press ctrl-Esc and then right-click on the viewer task icon to see the menu or. 
	Refresh screen
	Change the color quality
	Display in 256-bit color
	Enable agent computer's mouse and keyboard during remote controlling
	Disable agent computer's mouse and keyboard during remote controlling
	Allow using clipboard during remote controlling
	Prohibit to use clipboard

Table 8.9 Remote Control Panel Functional Buttons

Right click the remote control windows to send **Ctrl + Alt + Del, Ctrl-Esc** or **F12** commands to remote computer.

8.2.2 Remote File Transfer

Select target agent computer from the network tree, then select **Maintenance→Remote File Transfer** from menu bar or right click to select **Control→Remote File Transfer**. There are 2 types of authorization methods for remote control: agent user authorization and password authorization which are same as Remote Control (details please refer to Section 8.2.1)

Remote File Transfer Interface:

It includes menu bar, toolbar, local and remote view panels and status bar. Refer to the following figure 8.15, the left-hand-side panel is local view and the right-hand-side panel is remote view.

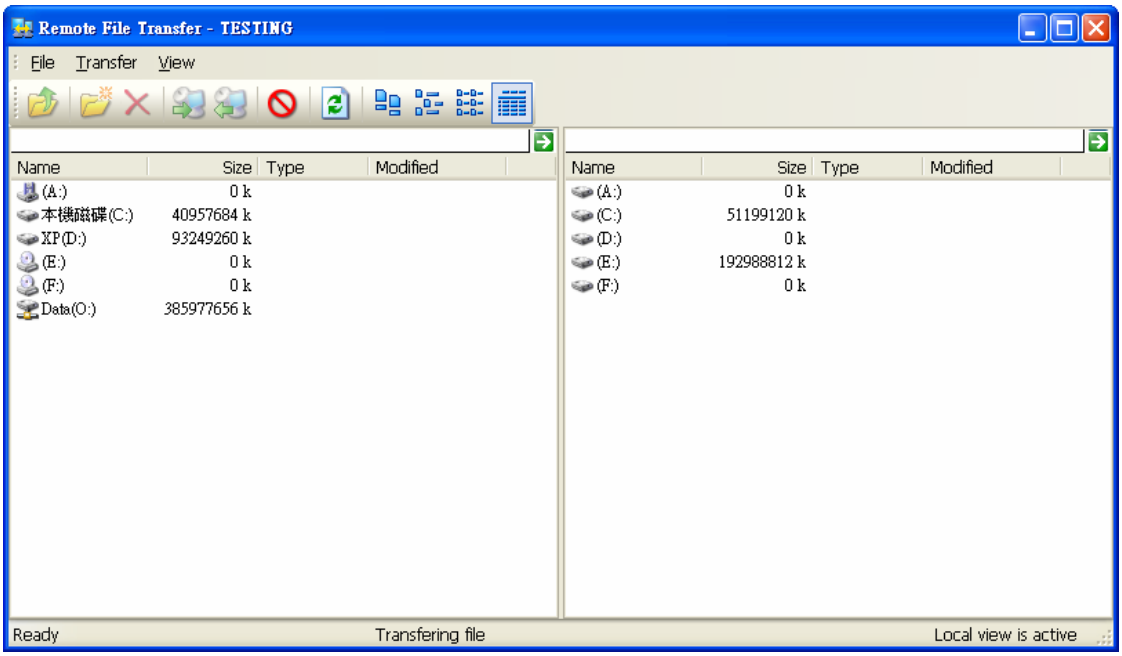


Figure 8.15 Remote File Transfer

File Operations:

System administrator can directly click the folder and access the following sub-folders or select **File→Up** to move up to previous level, also the folder or file path can be input in the address bar directly. Some basic file operations such as create, rename, delete are also available in this function.

File Transfer:

Local to Remote	Select the target files/folders from local and select the destination folder in remote side, and then select **Transfer→Local to Remote**, the file will be transferred from local to remote immediately. See the status bar to determine it is in local view or remote view and the file transfer status.
Remote to Local	Select the target files/folders from remote side and select the destination folder in local, and then select **Transfer→Remote to Local**, the file will be transferred from remote to local immediately. See the status bar to determine it is in local view or remote view and the file transfer status.
Terminate Transfer	Select **Transfer→Stop** to stop the transfer action. See the status bar to determine and the file transfer status.

Table 8.10 Remote Control Transfer Functions

Display mode:

Both local and remote view support Large  , Small  , List  and Details  icons.

Chapter 9 Assets Management

9.1 Assets Management

Assets Management collects all agent computers' software and hardware information to facilitate Enterprise to manage, audit and maintain their computer assets efficiently.

Select **Assets→Assets** to open the assets management windows. The window includes Title bar, Menu bar, Toolbar, Navigation bar, Data panel and status bar.

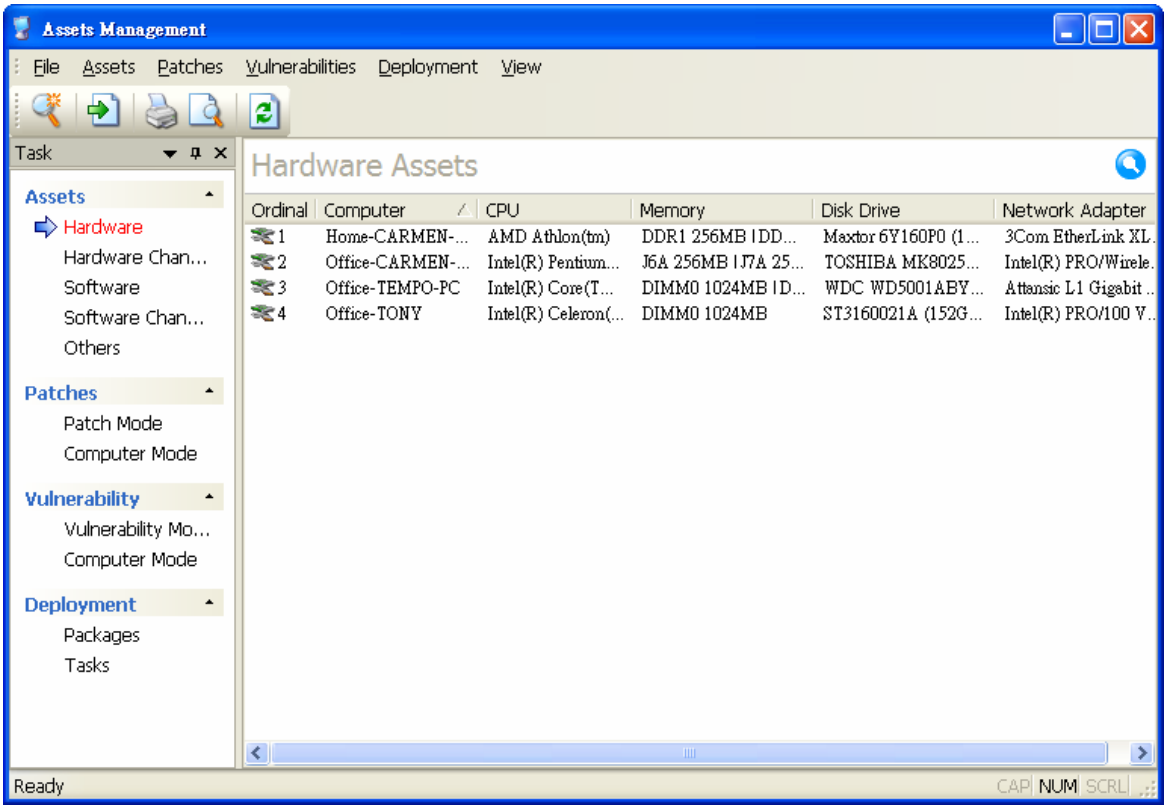
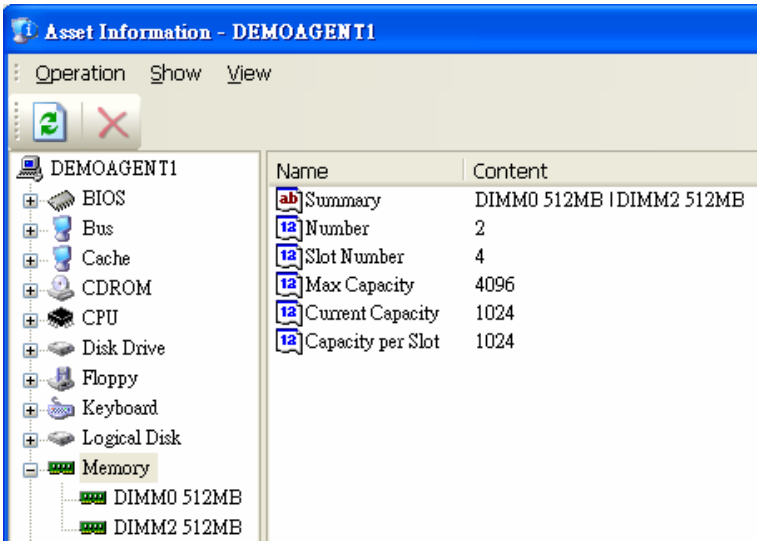
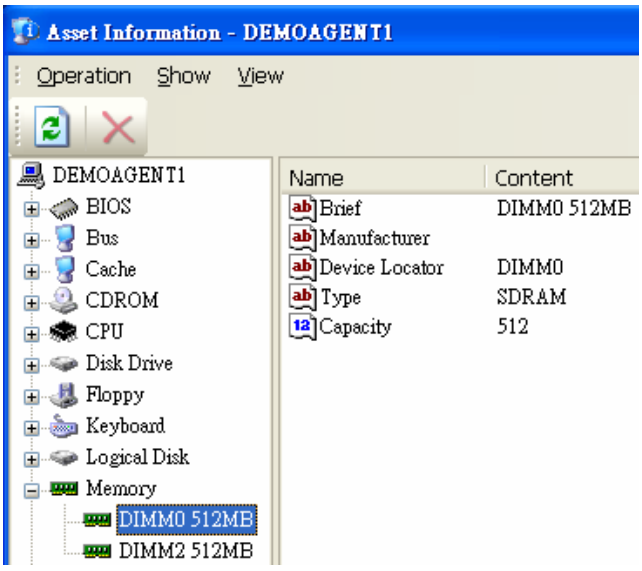


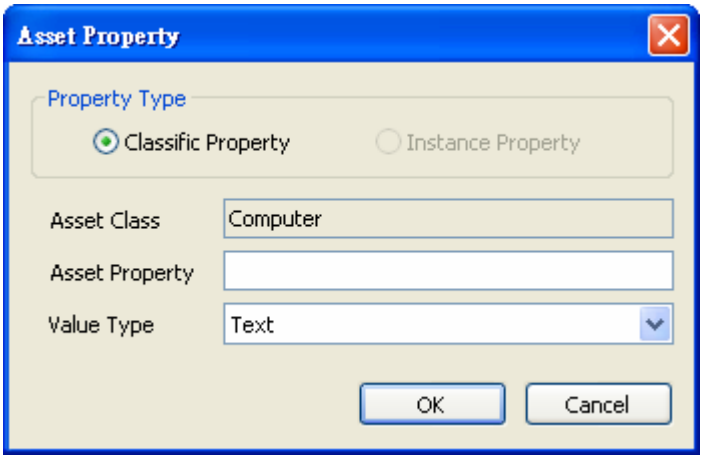
Figure 9.1 Asset Management

9.1.1 Assets Types and Property

Assets Types	
Assets types include computer, hardware, software and self-defined types	
Computer	Summary of agent computers such as logon user, domain and computer name etc.
Hardware	Hardware types such as CPU, memory, hard disk, motherboard, NIC etc.
Software	Software types such as Operating System, Application Software, Anti-virus program, Windows System Software and Microsoft Product Patches.
Self-defined	Self-defined assets types means which are customized by System administrators which may not be collected from agents automatically such as routers, printers, desk, chairs etc.

Table 9.1 Asset Types

Assets Property	
For every asset such as Memory, there are some properties to mention the details such as slot number, Max Capacity, Current Capacity, Capacity per Slot and Summary (DDR, SDRAM…) etc There are two types of properties: **Classific** Property and **Instance** Property	
Classific	Statistical properties of assets. For example, memory, a type of attributes such as the Current Installed Number of Memory, Slot Number, Max Capacity, Current Capacity and Capacity per Slot. 
Instance	Instance of asset class, for each memory it has attributes such as Device Locator, Capacity and Type etc. 
- if the asset class is Computer, it has only **Classific** Property	



- if the object is either Hardware or Software, both could have **Classific** and **Instance** Properties.
- All custom assets have only **Instance** properties.

Table 9.2 Assets Property

9.1.2 Assets Classes Management

All assets classes and their properties are listed in the assets class management, System administrator can use the Console to check the properties details or add any properties manually.

In the **Assets Management** windows, select **Assets→Asset Classes Management** to open the management window. In this window, the assets structure tree is placed in the left panel and the assets properties displayed in the right panel. In the properties list, the black color text represents **Classific** property and the blue color text represents **Instance** property.

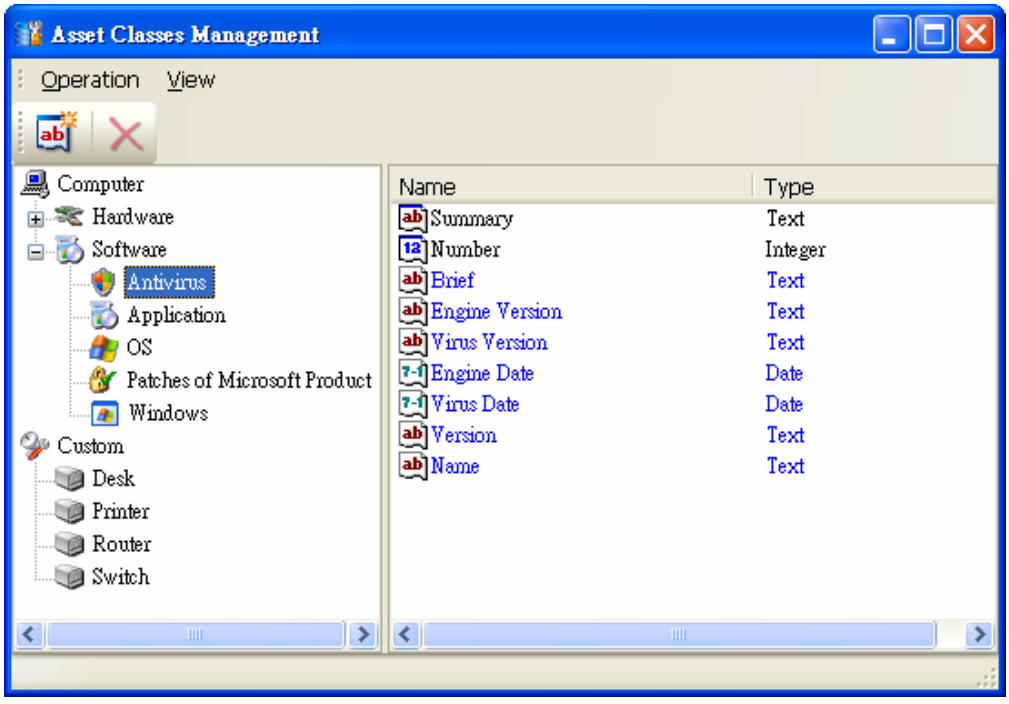


Figure 9.2 Assets Classes Management

Data Types of Property

There are 5 data types in asset properties, the followings are related icons to represent different data types	
	Text
	Integer
	Decimal
	Date
	Yes / No

Table 9.3 Data Types of Property

Custom Property

Except the System default asset properties, System administrator can add the property manually.

For example, how to add an Instance property in **CPU** class called **Repair date**.

- Select CPU in the asset tree in the left panel, then select **Operation→New Property** or click the button  to add property
- In the Asset Property window, check the **Instance Property** option, input **Repair date** in Asset Property field and select **Date** in the Value Type field. Click **OK** to confirm

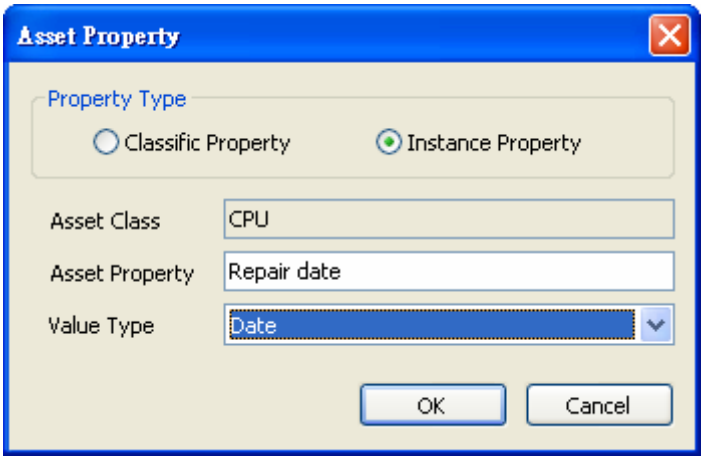


Figure 9.3 Asset Property

After the Instance Property is added, the property showed with * symbol. It represents it is custom property. All custom properties can be renamed (**Operate→Rename**) or deleted (**Operate→Delete**) but the default properties cannot.

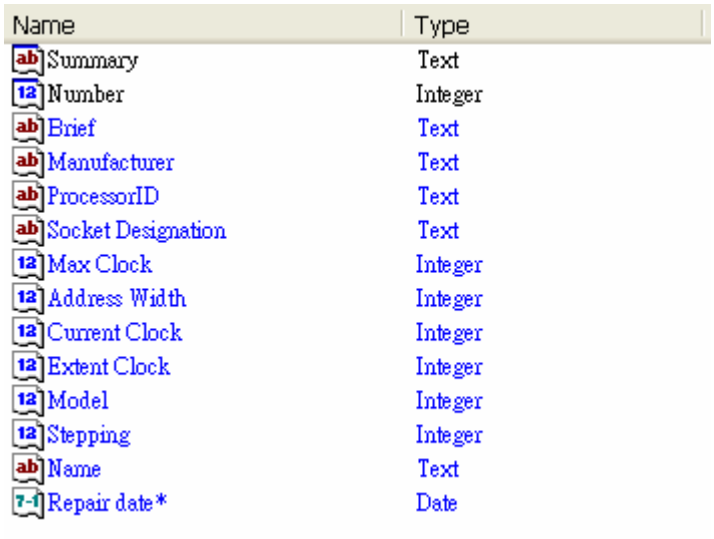


Figure 9.4 Asset Properties

Custom Asset

System administrator can custom asset to create a database to save all other assets information.

How to add a custom asset? e.g. office has 3 printers, System administrator can add a custom asset called Printer.

- Select **Operate→New Asset** to input **Printer** and then also add the corresponding Instance properties such as Model, Department, Buy Date, Price, Warranty etc.

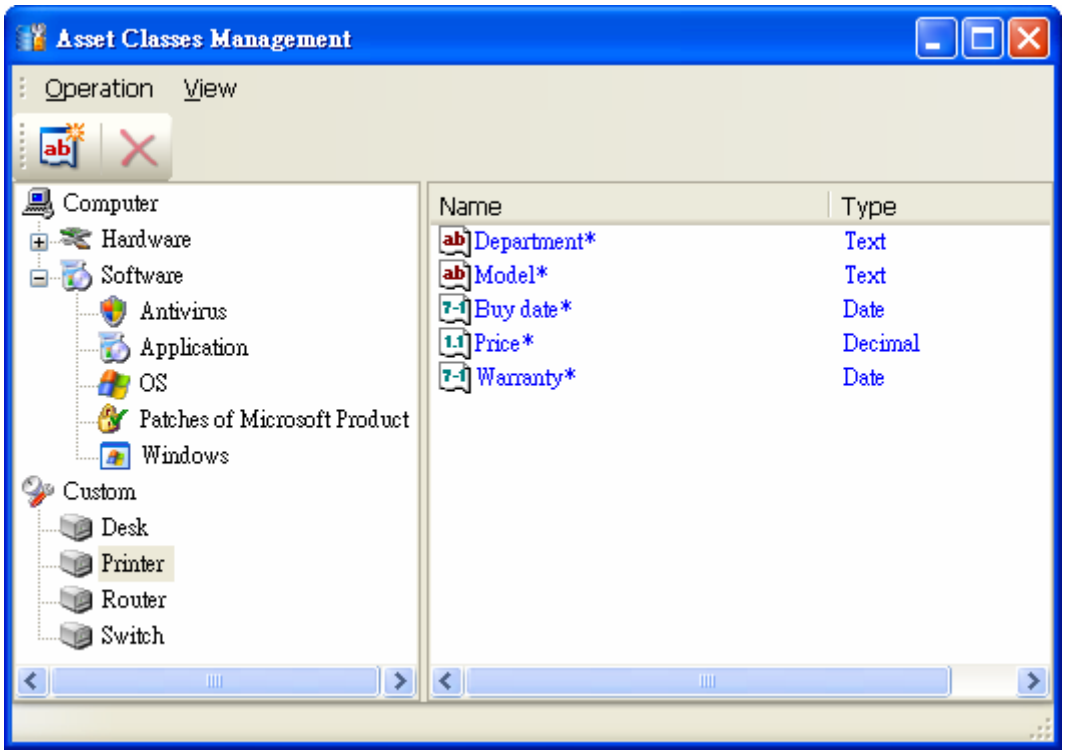


Figure 9.5 Custom Asset

For all custom assets, System administrator required to add the property value manually. Details please refer to Section 9.1.7

9.1.3 Hardware Query

Select **Assets→Hardware** to check all hardware assets of agent computers or input conditions to filter the query results.

Query Asset Information

By default, all agent computers CPU, Memory, Disk Drive and Network Adapter are listed. Double click one of the computers in the list to view the details of individual agent.

In the individual Asset Information windows, by default it shows the hardware information. Select **Show→All** or **Show→Software** to view other assets information.

In the asset property, there is a default property **Brief**, this information focus the asset Instance property. While in all classific property, there is a default property **Summary**, it shows the summary of all instances.

☞ **Hints:**

When viewing the asset information, the custom asset value can be added directly. Select **Operation→New Property** to open the Asset Property window to add the asset property values.

Query Conditions

Click the button to open the Query Conditions windows, System administrator can set one or more query conditions to filter the results

Range	By default, it is set to **{The Whole Network}**. Select button to specify the target group
	Click this button the **Conditions** windows opened. Each condition includes: asset properties and logic e.g. Memory-Number == 2 or CPU-Name include AMD
	Delete existing conditions
	View and edit existing condition

Table 9.4 Query Conditions

Caution

Query conditions of Instance Property and Classific Property

If a condition includes asset A's Instance property first, the following conditions cannot include another Asset B's Instance properties (all other Instance properties will be hidden automatically), in this case only classific property conditions can be added for the followings input conditions.

Result List

After input required conditions, asset properties are then added to the Result Lists:

=>	Double click the property from the left panel or click this button to add the property to result list
<=	Double click the property from the right panel or click this button to remove the property from result list

Table 9.5 Result List

Caution

Query conditions of Instance Property and Classific Property
Same as query, if a condition includes asset A's Instance property first, the following conditions cannot include another Asset B's Instance properties (all other Instance properties will be hidden automatically), in this case only classific property conditions can be added for the followings input conditions.

Save / Delete Query Settings

To facilitate the query, the settings can be saved after completing the conditions input

Save	In the Query windows, input the Name and click this Save button to save the current query. Select from the drop-down menu to select the saved query.
Delete	Click this Delete button to delete the saved query
Set Default	Click this Set Default button to set the current query as default. Next time when open the Asset Management windows, the default query results will be displayed.

Table 9.6 Save / Delete Query Settings

Add Custom Property Value

According to the previous example CPU-Repair date, set a query condition: CPU-repair date Not exist and the result lists include: Computer-Summary, CPU-Brief and CPU-Repair date. The resulting query shows that the CPU-Repair date is empty. If you want to add the Repair date, click the CPU-Repair date column, the field becomes editable. Now you can add the value one by one.

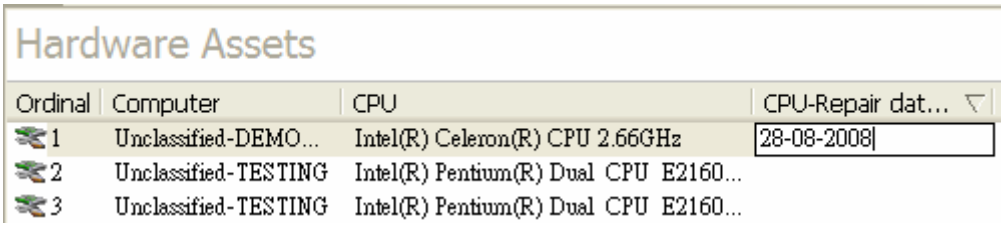


Figure 9.6 Hardware Assets

Caution

Add the custom properties
The result list must include CPU-Repair date, also any one of the CPU instance properties must be included. Otherwise, the property value may not be added. The reason is that CPU-Repair date belong Instance property, we cannot add the same value for all instance properties for a computer.

9.1.4 Hardware Change

Hardware Change log all hardware changes made from agent computers including **add**, **delete** and **change**. Select **Assets→Hardware Changes** to view the hardware changes log.

Hardware Change Contents

The contents include: Type, Time, Computer, Asset and Description	
Type	Type of asset change: Add, Delete or Change
Asset	Asset classes such as CDROM, CPU BIOS etc.
Description	More detailed information about the asset shows in this column

Table 9.7 Hardware Change Contents

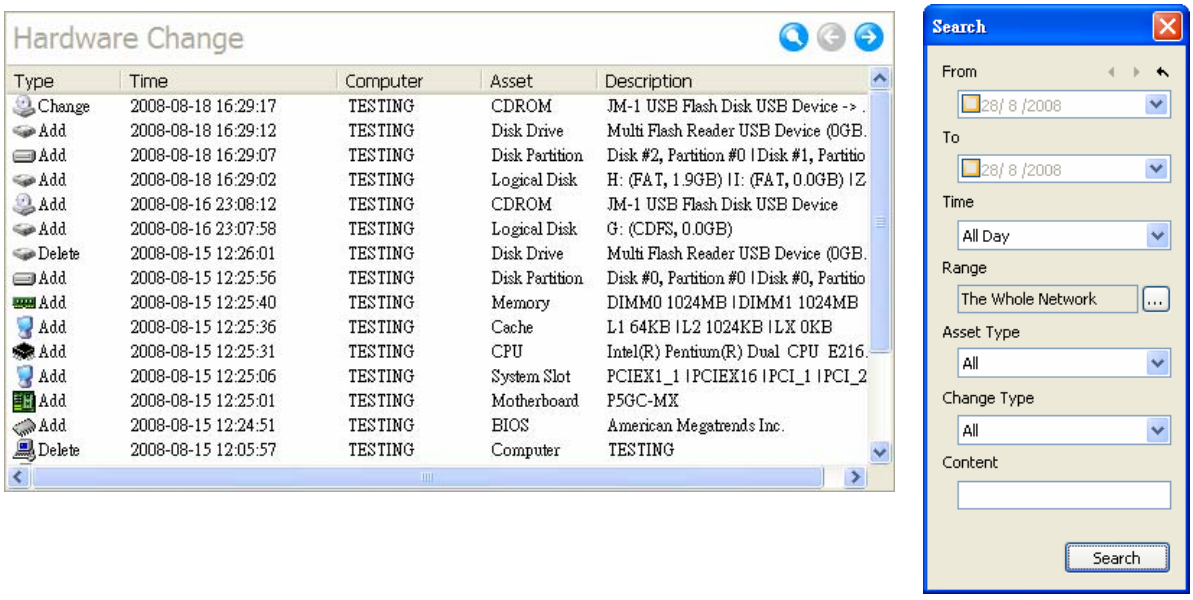


Figure 9.7 Hardware Change

Query Conditions

Select **File→New Query** to open the search panel, System administrator can set different conditions to filter.

Time & Range	Common query conditions
Asset Type	By default, it is set to All. Select Asset Type from the drop-down menu to specify the type to filter the query result.
Content	Specify asset contents. Support wildcard input.

Table 9.8 Hardware Change - Query Conditions

9.1.5 Software Query

Select **Asset→Software** to switch to the software asset. By default, the query is Computer and Operating System, System administrator can set other query condition to query the required results. The software query method is similar to Hardware Query, please refer Section 9.1.3 for details.

9.1.6 Software Change

Software Change log all software change made by agent computers including add, delete and change. Select Asset→Software Change to check all software change logs.

The software change log contents include: Type, Time, Computer, Asset and Description which are similar to Hardware Change.

Query Conditions

Time & Range	Common query conditions
Asset Type	By default, it is set to All. Select Asset Type from the drop-down menu to specify the type to filter the query result. It includes Operating System, Application, Antivirus, Windows and Patches of Microsoft Products.
Content	Specify asset contents. Support wildcard input.

Table 9.9 Software Change – Query Conditions

9.1.7 Other Assets

System administrator required to input the asset property values after completing the custom asset management.

Add Custom Asset

According to the previous Printer example, select **File→New Query** to open the Query Condition window. Query conditions are empty and the result includes Printer- Model, Printer-Department,

Printer-Buy date, Printer-Price, all of these properties will show in the results.

Click the add button  to enter the property's value one by one to record the Printer information.

Query Custom Asset

After completing to add the asset and its properties, System administrator can create query condition. Select File→New Query to set the conditions e.g. Printer-Price >= 1000 and the result list includes: Printer-Model, Printer-Department, Printer-Buy date, Printer-Price. The resulting query will only show the printer which the price is above or equal to 1000.

9.2 Patches Management

Patch Management function scans all patches status of all agent computers and based on the agent computer requirements to install patches automatically and manually to enhance the security.

Patches Scanning, Download and Install

The patches updater is running on the IP-guard server, it will automatically download and update the patch scanning file (wsusscan.cab). This file will be downloaded to agent computer after the agent program installed in client computer at the first time.

Select **Asset→Patches** to check the agent computers patches situation. Also, System administrator requires to set the download policies to download the patches to the server and then install patches to agent computer. Agent computers base on the server settings to get the patches file and process the installation automatically.

☞ **Hints:**

Combine the use of **CTRL** and **SHIFT** keys to set the download policies for multiple patches or computers.

Control functions

System administrator can set the order of download scanning file or patches in the COnsole	
Download Scanning File	Click the button  to select the option **Download Scanning file**, server will download the latest scanning file immediately.
Download All Patches	Click the button  to select the option **Download All Patches**, server will download the required patch files immediately.
Scan Now	Click the button  to select the option **Scan Now**, all agent computers will scan the patch once immediately.
Scan for system patches	If only one agent computer to scan the patch, right click the computer and select **Scan for system patches**, then only the specified computer will be scanned.
Computer Range	Click the button  to select group or individual computer to check the patch

	installation situation.

Table 9.10 Control Functions

9.2.1 Patch Mode

Patch Log Contents

Under Patch mode, all patches scanned from agent computers will be listed including Ordinal, Severity Rating, Bulletin ID, Patch ID, Name, Not Installed, Auto downloading and Download Sate	
Severity Rating	5 different ratings: Low, Moderate, Important, Critical and Unknown
Bulletin ID	Microsoft Published Bulletin ID
Patch ID	Patch ID
Name	Patch Name with ID
Not Installed	The total number of agent computers not installed the corresponding patch. Select the patch to check the installed / not installed patch situation from the bottom panel.
Auto downloading	System administrator can set the download policy: Download or Not Download. By default it is set to Not Download and this field is blank, server will not download the patch automatically.
Download State	Includes Not Download, Download or Downloaded. When mouse moves to the column, the download status will be displayed in %. Complete download will show as 100%
Detailed Information	Double click the patch or right click to select Details to check more information about the patch including Download Path, Size and Description etc.

Table 9.11 Patch Log Contents

Patch Download Settings

Under Patch mode can check all agent computer patches list, By default, system would not install and install the patches automatically, System administrator required to set manually.

In the Auto Downloading field, using ✔ to represent that patch is set to Download; if set to Not Download, this field is empty and the server would not automatically download.

For the coming new agents, System administrator can set the patches download option automatically or not from the Console: select **Tools→Options→Server Settings→Patches**, there are two options there: **Install patches on new agents automatically** and **Download new patches automatically**. By default, these two options are not checked.

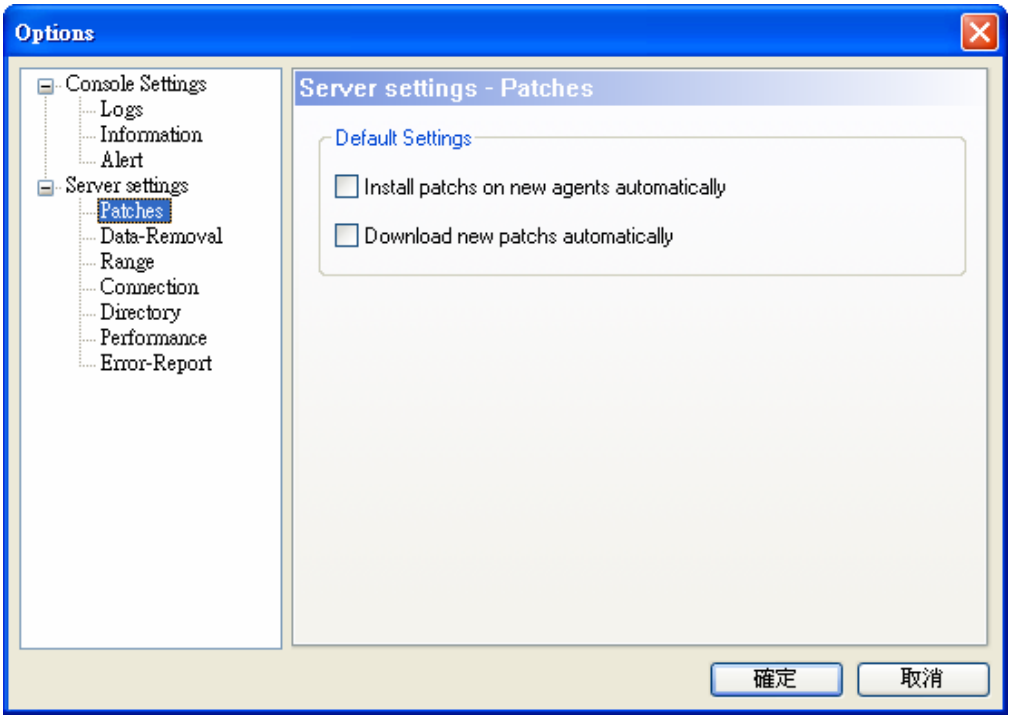


Figure 9.9 Options - Patches

9.2.2 Computer Mode

Computer Mode Contents

Under computer mode check all agent computers information and patches installation situation including Computer, IP address, Operating System, Last Scanned Time and Auto installing	
Computer	Agent Computer belonging group and computer Name
IP address	Agent computer IP address
OS	Agent computer Operating System
Last Scanned Time	The last scanned patch time of the agent computer
Auto Installing	Auto install or not

Table 9.12 Computer Mode Contents

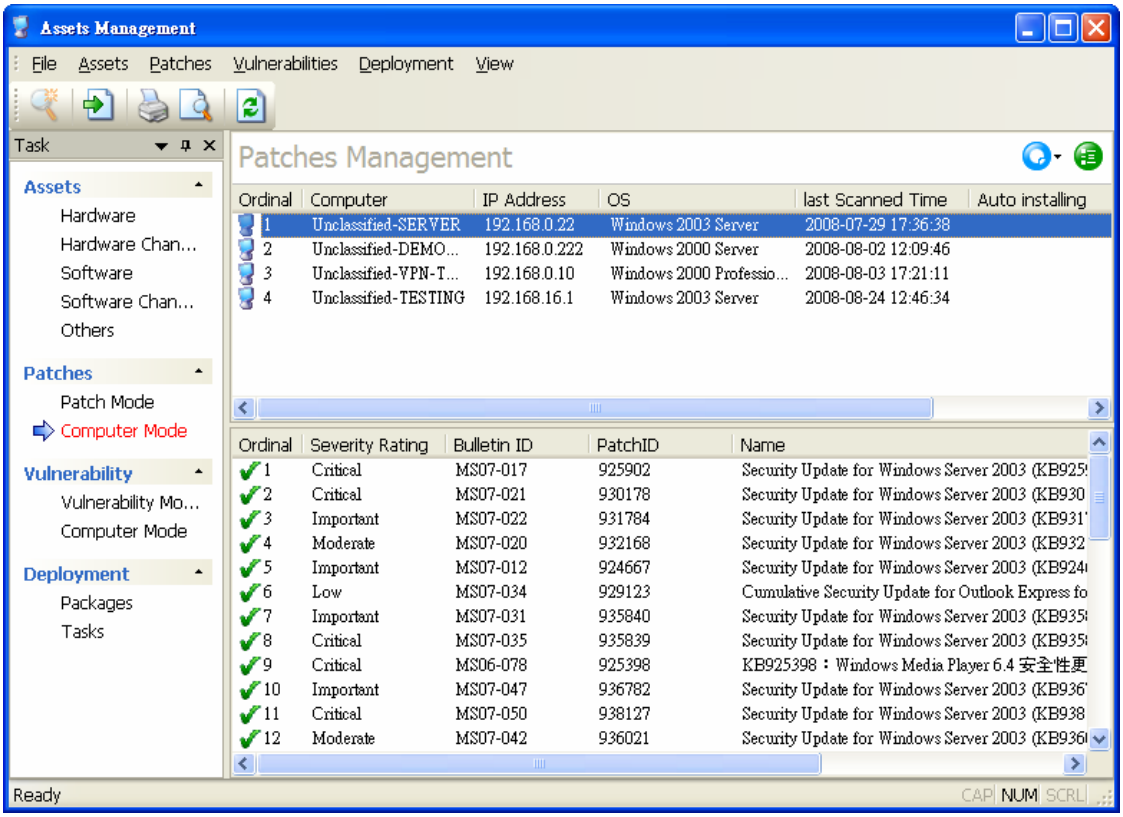


Figure 9.10 Patch Management – Computer Mode

Computer Patch Install Setting

Under Asset Management, select **Patches→Computer Mode**, it shows the agent computer list and the details of patches installation. By default, the patches download and installation are not automatically, System administrator required to set the settings manually.

Select one of the computers to right click to set **Install** or **Not Install**, agents set with **Install** the patches will be automatically downloaded and installed while agents set with **Not Install** will not do anything.

In the detailed list of patches under computer mode, System administrator can specify patches to download for individual computer. Select the desired patches (using CTRL key for multiple selections) and then right click to set **Install** or **Not Install**.

For the coming new agents, System administrator can set the patches download option automatically or not from the Console: select **Tools→Options→Server Settings→Patches**, there are two options there: **Install patches on new agents automatically** and **Download new patches automatically**. By default, these two options are not checked.

9.3 Vulnerability Check

Vulnerability check function automatically scans the internal network computers and process analysis to help System administrator to check and trace the vulnerability problems. Follow the resulting suggestion to take timely response measures to enhance the security of all internal computers.

Under Asset Management, select **Vulnerabilities→System Vulnerabilities** or **Computer Mode**, click the vulnerability management button  to execute the vulnerability scanning immediately. Click the computer button to view a computer group or individual computer vulnerability information.

9.3.1 Vulnerability Mode

Under vulnerability mode (**Vulnerabilities→System Vulnerabilities**) can check the list of vulnerability information of corresponding agent computers. The list includes the following information: Ordinal, Severity Rating, Name, Vulnerability, Pass and other detailed information.

Severity Rating	3 different ratings: Information, Normal and Critical
Name	Summary of the vulnerability
Vulnerability	Total number of agent computers having the corresponding vulnerability
Pass	Total number of agent computers having no vulnerability
Other detailed information	Double click any vulnerability from the list to see the details. Apart from the details of the vulnerability, system also provides solutions for System administrator to solve the particular vulnerability problem.

Table 9.13 Vulnerability Mode

9.3.2 Computer Mode

Under Vulnerabilities→Computer mode to view and check the agent computer information and corresponding vulnerability information including Computer, IP Address, OS, Last Scanning Time and Auto Installing. Double click any vulnerability from the list to see the details and find out the suggested solutions.

9.4 Software Deployment

System administrator can install software, run an application, and deploy files to agent through IP-guard console. Software can be installed to the agent by simply creating a deploy task. System administrator can view the deployment status from the console. With the software deployment function, System administrator also can organize and deploy software to the networked agent computers more efficiently and consistently.

Select **Assets→Deployment** for software deployment. Deployment is divided into two steps: packages creation and tasks creation.

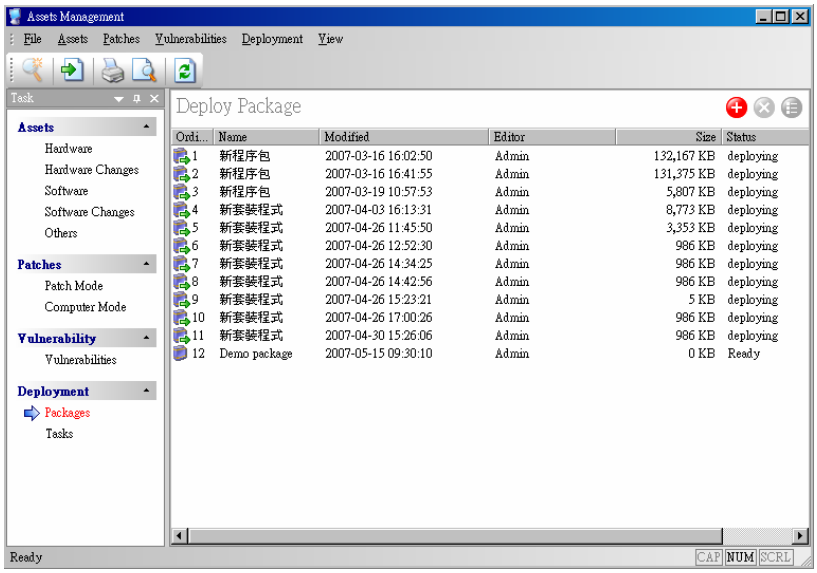


Figure 9.11 Deploy Package

9.4.1 Package Deployment

System administrator requires creating a deployment package first, deployment package includes required deployment conditions which can be saved in server and used repeatedly.

Click the new button  to create a new package or right click deploy package list to new one, the deployment conditions include: **General conditions**, **File Conditions**, **Checkup conditions** and **Necessary conditions**.

General Conditions Settings

Input basic information: package name, operating system, and language	
Name	By default, it is set as **New Package**. System administrator can rename it but cannot be empty
Created and Modified Time	These two fields will be generated by system and cannot be edited. They are empty when the deployment package is still in creating. Once completed, the created time and System administrator name will show. Any changes made of the deployment task, the modified time will also be

	updated.
Operating System	By default, all are selected. System administrator can select the target Operating System for the deployment
Language	By default, it is set to **All**. System administrator can select the target language from the drop-down menu.

Table 9.14 Package General Condition Settings

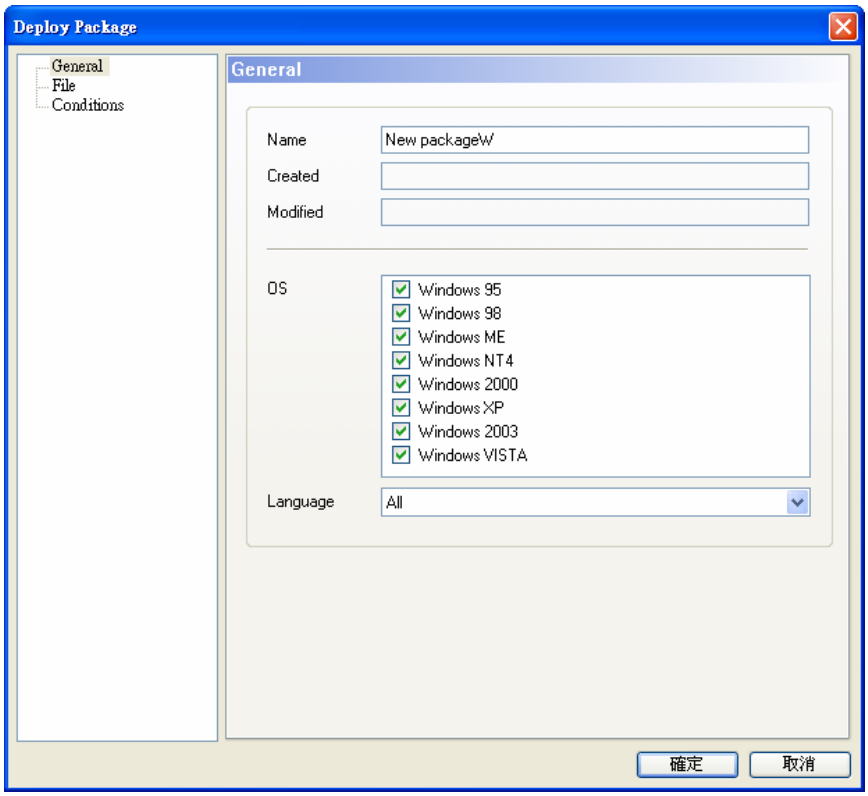


Figure 9.12 Deploy Package General Condition Settings

File Conditions Settings

From the left panel select **File** to switch to File Conditions Settings

General	
Size	The size can be checked after successful creation of the deployment package
Computer	The computer used to create the deployment package using Console
Path	The complete file path
Parameters	
Command	This command parameter is used to install software or execute program during package mode. There are two methods to input this field: 1) right click the software installation item from the File List to click Copy to Command-Line (see the following figure) or 2) Input the name manually.

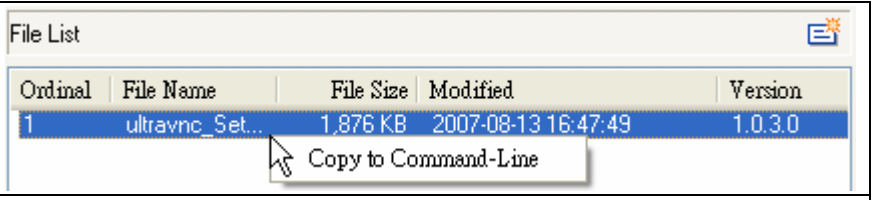
		
Deploy Mode		There are three modes: Install, Execute (once) and Deploy File
	Install	Distribute application software installation program to agents and process installation.
	Execute (once)	Execute the distributed program once only in agent side.
	Deploy File	Deploy file(s) to agent, the default destination path is {sd}\deploy files, it can be changed manually. Notes that {sd} means System Drive, if OS is located in D:\windows, it is D: More details please refer to the following table 9.19.
Run Mode		Run mode means there are some interactions required between the installation process and the user; user should be able to see the installation and execution interface during installation. If this option is not checked, it means it is silent installation – user cannot see the installation and execution process. However if the program itself does not support silent mode installation, it may cause installation failure.
File List		Click the button to select required file(s) (or folder), if multiple files are selected, they must be placed in the same folder. Every time click the button to create a new file list which will automatically override the previous created file list. The information of the file list includes: File Name, File Size, Modified and Version

Table 9.15 Deploy Package File Condition Settings

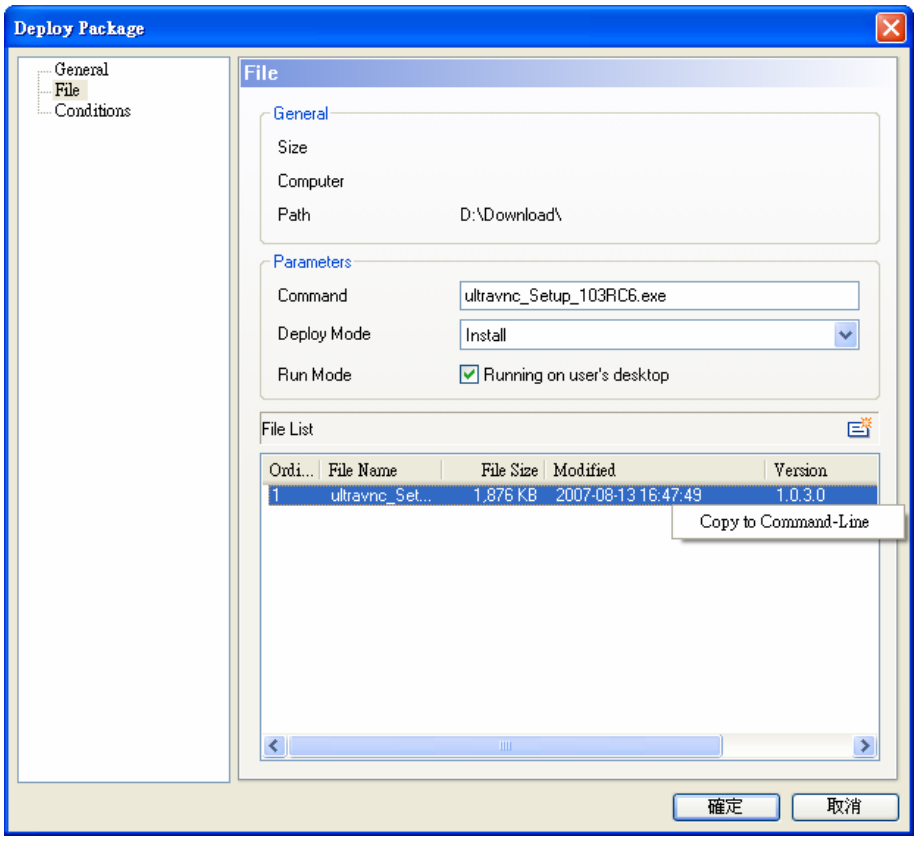


Figure 9.13 Deploy Package File Conditions

Checkup conditions and Necessary conditions

1. Purposes of Checkup conditions and Necessary conditions

Checkup conditions	Only enabled under Install mode. The checkup conditions are used for agent to check the required installation conditions. Once satisfied, agent will install the program automatically.
Necessary conditions	Prerequisite checking before distributing programs or files. Once satisfied, all specified files or programs will distribute to agents. Otherwise, no actions taken.

Table 9.16 Purposes of Checkup conditions and Necessary conditions

2. Setting of Checkup conditions and Necessary conditions

There are 5 types in checkup conditions: File, File Version, RegKey, RegValue and Installed software	
File	Determine the file exists or not, required to input complete path
File Version	Determine the file and its version, required to input complete path
RegKey	Determine specified register key exists or not
RegValue	Determine specified register value exists or not
Installed software	Normally the installed software means that windows **Control Panel → Add / Remove Programs**

Table 9.17 Settings of Checkup conditions and Necessary conditions

Example of Checkup Conditions: Install Office 2003

File	Exist "%pf%\Microsoft Office\OFFICE11\EXCEL.EXE"
File Version	>= "%pf%\Microsoft Office\OFFICE11\EXCEL.EXE" "11.0.5612.0"
RegKey	Exist "SOFTWARE\Microsoft\Office\11.0\Access\InstallRoot"
RegValue	Exist "SOFTWARE\Microsoft\Office\11.0\Access\InstallRoot" "Path"
Installed software	Include "Microsoft Office Professional Edition 2003"

Table 9.18 Example of Checkup Conditions

☞ **Hints:**

The followings are the system default shortcut using in conditions input:

"tmp"	temp folder (c:\windows\temp)
"win"	windows directory (c:\windows)
"sys"	system directory (c:\windows\system32)
"pf"	program files (c:\program files)
"sd"	system drive (c:\)
"cf"	common files (c:\program files\common files)

Table 9.19 Default Shortcut Conditions Input

Other Operations:

	Delete package. Only the package with the status can delete.
	Edit packet. Only the package with status can edit
View	The basic information includes: Name, Modified, Editor, Size and Status. Double click to see the details

Table 9.20 Other Operations

 **[Important]**

About Package Task...

1. Make sure all files and folders for the installation package are located in the same folder and select the required files at once. It is considered as a new file list and replaces the existing on every click of  .
2. When deploy mode is install or execute (once), select the main file in command line. When deploy mode is deploy files, select the destination path for the files to deploy to.
3. The default run mode is to run on user's desktop which will interact with users during the installation process. User will not be able to see the installation process if this option is unchecked.

9.4.2 Task Distribution

Except to create distribution packet, tasks distribution is also required to create to specify target agent computers. Click the button to create a task.

Task distribution settings include: Task Name, Package Name, Max Retry and Target computers.

Task Name	By default, it is set to New Task. System administrator can edit the name but it cannot be empty
Package Name	Click the button to select required package which created in package part
Max Retry	The task will retry if it is failed. Be default, it is set to 10. if 0 is input, it means unlimited retry
Target	Click the button to select target agent computers

Table 9.21 Task Distribution

Click OK will start the deploy task immediately. Select the task to view the task status. Task cannot be deleted when deployment. User can right click on the task and select stop to stop the task. Right click on a computer and select Cancel to cancel the task on the computer.

	Delete task distribution. Task cannot be deleted when deployment. User can right click on the task and select stop to stop the task. And then delete the task.
	Edit task distribution. Task cannot be edited during deployment. User can right click on the task and select stop to stop the task. And then edit the task.

Table 9.21 Task Distribution Operations

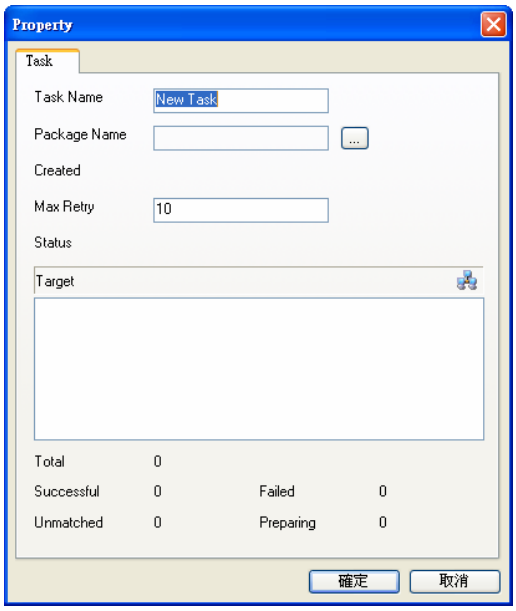


Figure 9.14 Task Distribution Properties

Caution

Deploying...
If the task status is **Deploying**, it cannot be deleted or edited, only delete the distribution tasks the corresponding package status would change to **Ready**.

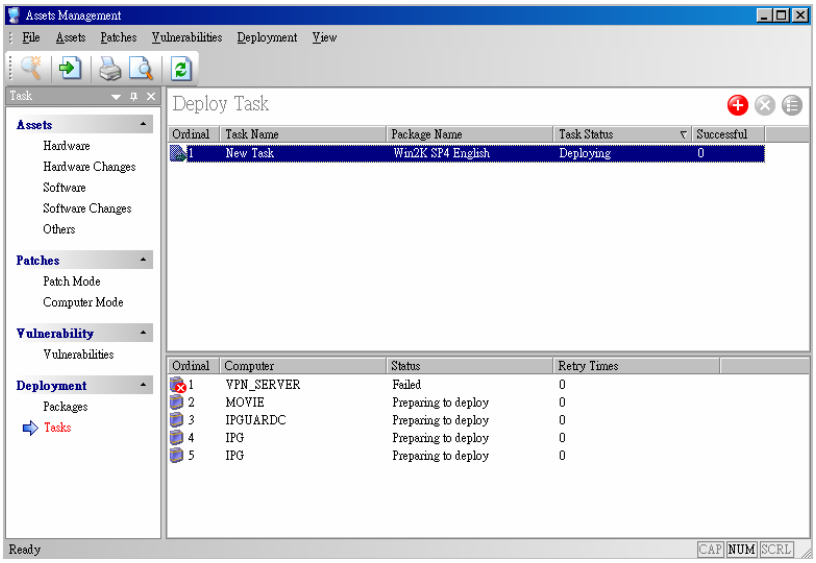


Figure 9.15 Deploy Task

Chapter 10 Intrusion Detection

The Intrusion Detection function in IP-guard is used to discover any illegal or unauthorized computers accessing Enterprise' internal network and then apply corresponding policies to block their communications with internal network.

10.1 Startup Intrusion Detection

To start the Intrusion Detection settings, go to **Tools → Intrusion Detection** (see Figure 10.1)

At the first time, no computers display in the **Intrusion Detection windows**. Select **Operation → Setting…** to set the Intrusion Detection settings.

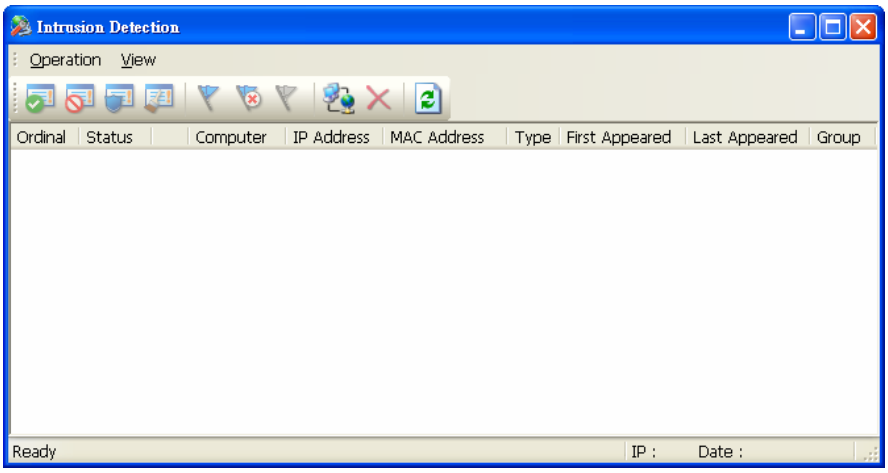


Figure 10.1 Intrusion Detection windows

In the **Setting** windows (see Figure 10.2), check the **Enable intrusion detection** option. Here are two cases would happen either input the IP address range or not::

Case 1: Without specify IP address range

- All online computers (agent and non-agent computers) are scanned and listed out if each subnet at least has a computer installed with agent.
- In each subnet, IP-guard automatically assigns one computer to be representative to manage all computers within that subnet. The representative computer so-called **Intrusion Detection Agent** indicated with red flag

Case 2: Specify IP address range

- If IP address ranges are set, IP-guard only scans the computers within those ranges. Make sure that at least one IP-guard agent installed in each specified range. Otherwise, no computers can be scanned out from that range.

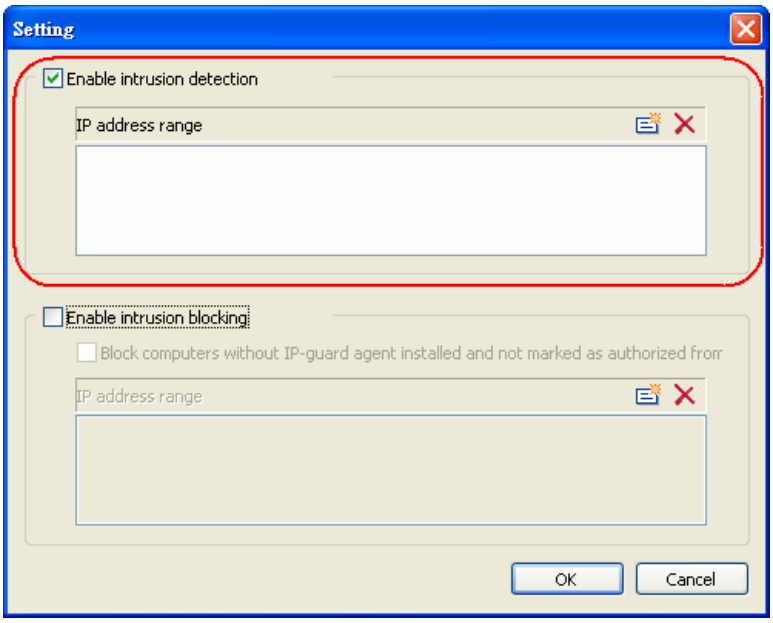


Figure 10.2 Setting windows

If the computers are already listed in the Intrusion Detection main windows, there will be no alert message if it offline and then online again. However, alert message will popup if new computers are discovered (see Figure 10.3)

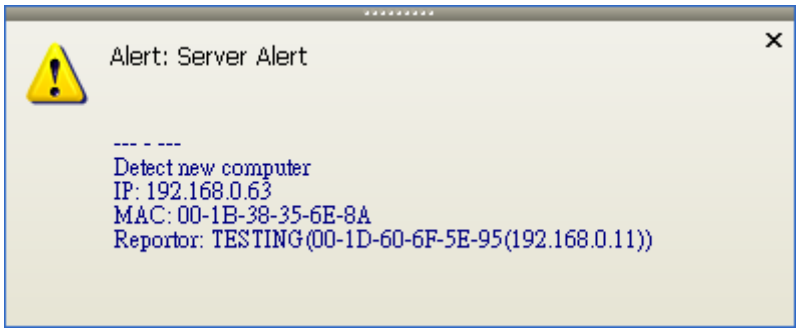


Figure 10.3 New computer detected alert message

Computer Types and Settings

By default, there are 2 types classified when computers discovered: **Normal** and **Unknown**

Normal	- It represents the computer installed with IP-guard agent
Unknown	- It represents the computer without IP-guard agent installed and does not specify the type manually. - if options **Enable intrusion blocking** and **Block computers without IP-guard installed and marked as authorized…** are selected in the setting, the unknown type computers are treated as **illegal type computer**. Treated as illegal computers, all communications between illegal type computers and protected type computers are blocked.

Table 10.1a Computer Types and Settings (Default)

Except **Normal** and **Unknown** types, there are 3 more types can be set manually including **Authorized**, **Protected** and **Illegal**, the functions descriptions are listed as following table:

Authorized	- All communications will not be blocked if computer treated as Authorized type - What kinds of computers should be set as Authorized such as Department Heads' computers which may not install IP-guard agent, and some key network devices such as switch and router (e.g. router A's IP address is 192.168.0.1), should also be set as Authorized. This setting can prevent they are treated as illegal as they do not install IP-guard agent
Protected	Generally some important computers such as File Server, Database Server etc. are set as **Protected**, this settings can prevent the illegal computers trying to access confidential data.
Illegal	When **Enable intrusion blocking** function is activated, all communications between illegal computers and protected computers will be blocked.

Table 10.1b Computer Types and Settings (Manual)

☞ **Hints:**

Press **Ctrl** key for multiple selections of computers applying the same type settings.

10.2 Startup Intrusion Blocking

Enable Intrusion Blocking

After the above settings done in Section 10.1 completed, now the Intrusion Blocking can be enabled. Select **Operation → Setting…** The Setting windows will popup (see Figure 10.4) and the functions descriptions are listed in Table 10.2

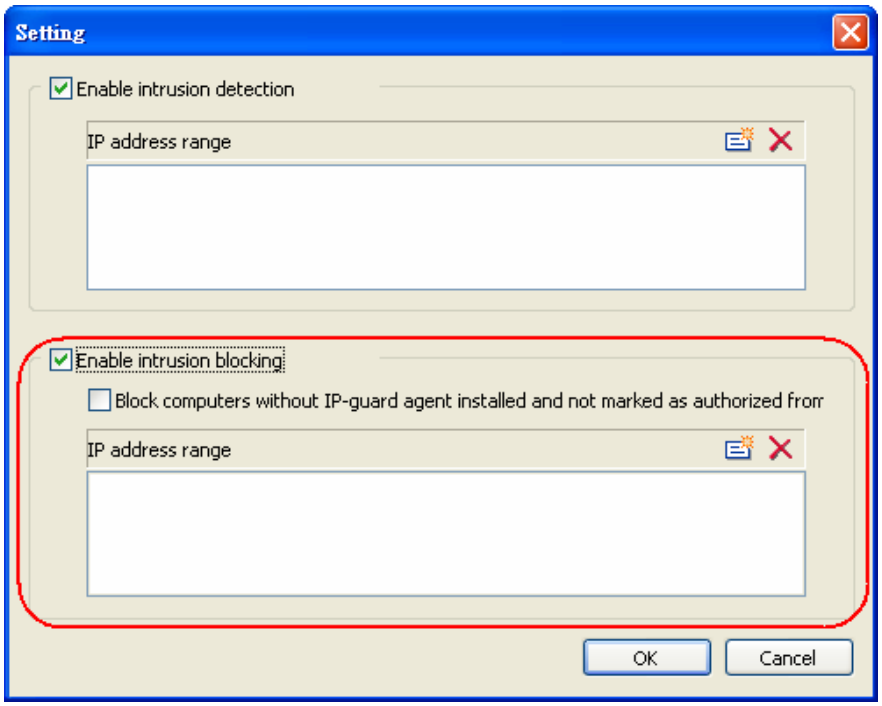


Figure 10.4 Enable Intrusion Blocking

Enable Intrusion Blocking	If this option is checked, the **Intrusion Detection Agent** will enable the intrusion blocking function to block the communications between **Illegal type computers** and **Protected type computers**
Block computers without IP-guard agent installed and not marked as authorized from Protected computers	If this option is checked, all **unknown type computers** are also treated as Illegal. In other words, these unknown type computers also cannot communicate with Protected type computer. **[Important]** - Before enable this function, make sure the unknown type computers are required to be blocked. Otherwise, set the specified type: Authorized or Protected manually. - Warning message will be given before confirm to enable this function (see Figure 10.5)
IP address range	- If no IP address range is specified, the **Intrusion Detection Agent** will block all illegal type computers' communication.

- if IP address range is specified, the **Intrusion Detection Agent** will only block the illegal computers' communications within the specified range

Table 10.2 Intrusion Blocking Functions

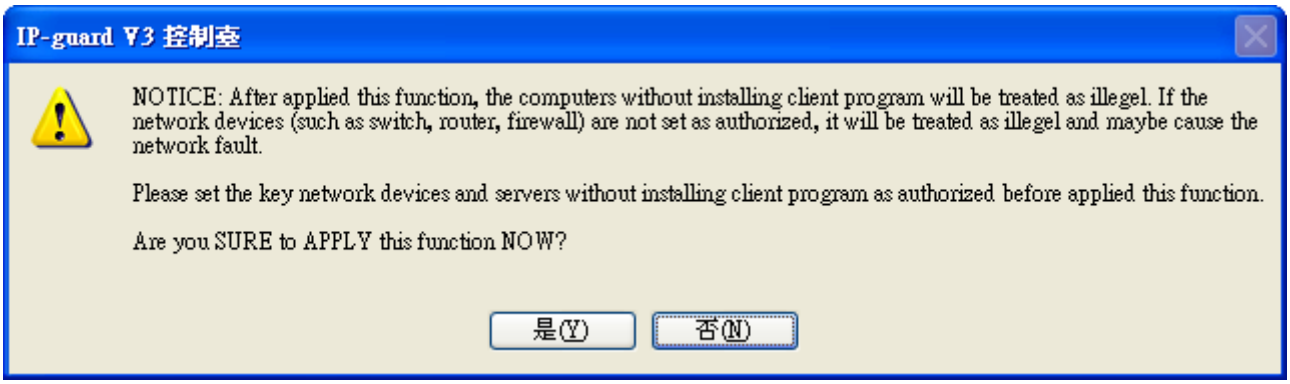


Figure 10.5 Intrusion Blocking Warning message

10.3 Other Setting Functions

10.3.1 Intrusion Detection Agent Selection

The computer indicated with red flag represented as **Intrusion Detection Agent**, this agent is responsible for scanning its belonging subnets' online computer and executing corresponding policies to block all illegal type computers' communication in the network.

To facilitate System Administrator to manage all computers, administrator can select one or more than one stable computers (e.g. a computer does not install with Firewall and not always power off) to become **Intrusion Detection Agent** so that one of them would be assigned to become **Intrusion Detection Agent**. Select **Operations → Set to detect agent**, represented as . Only **Normal type** computers can be set to be **Intrusion Detection Agent**.

System administrator can specify computers that they cannot be **Intrusion Detection Agent**. **Select Operation → Not to be detect agent**, represented as

[Important]

About Intrusion Detection Agent
- Only one **Intrusion Detection Agent** appears in each subnet - Set with **Set to detect agent** only means that those computers have higher priorities to be **Intrusion Detection Agent**, IP-guard system would make the final decision which computer becomes **Intrusion Detection Agent** but you have right to select which computers cannot be **Intrusion Detection Agent**.

10.3.2 Pre-defined Computer and Type

Except the computers scanned by **Intrusion Detection Agent**, System administrator can add a new computer manually and also preset the type for pre-control purpose. Select **Operation → Add** to add computer. (see Figure 10.6) Administrator can set IP-MAC type or either IP or MAC type (see Figure 10.6), the functions are described in Table 10.3.

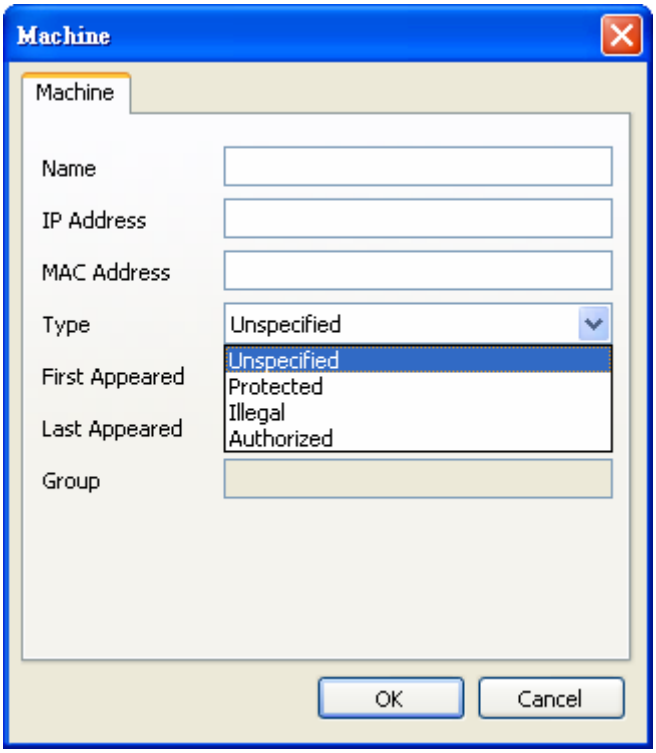


Figure 10.6 Add a New Computer

IP-MAC	A computer specified with IP, MAC address and type. If this computer is scanned, the type will be automatically updated to predefined type.
IP	Only specified with IP address and type. If a computer (without type setting) scanned that matched with pre-defined computer, then the type will be updated to pre-defined type automatically For example, pre-defined IP address 192.168.1.1 set as authorized. Once the computer (IP address is 192.168.1.1) scanned out, whatever the MAC address is, this IP address is set to be authorized.
MAC	Only specified with MAC address and type. If a computer (without type setting) scanned that matched with pre-defined computer, then the type will be updated to pre-defined type automatically For example, pre-defined MAC address 00-F0-4C-8C-DE-6A as Illegal. Once the computer (MAC address is 00-F0-4C-8C-DE-6A) is scanned out, this MAC address is set to be illegal.

Table 10.3 IP-MAC Settings

10.3.3 Search and Delete Computers

In the Enterprise Network, there must be many computers to be managed, for fast searching the target computer, System administrator can use searching engine to assist. Select **Operation → Find**, the **Find** dialogue popped up as following figure.

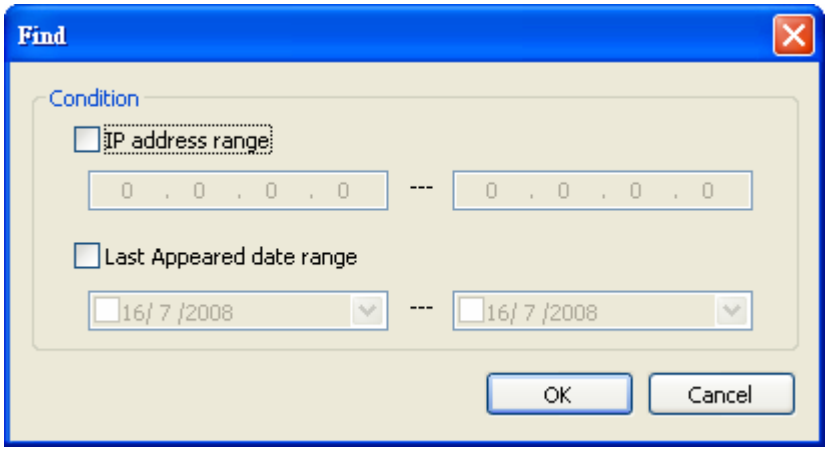


Figure 10.7 Searching Computers

There are 2 conditions: **IP address range** and **Last Appeared date range,** all computers within the specified range and last appear date range matched will be listed in **Intrusion Detection** windows

For some computers not used for a long time, it can be deleted from **Operation → Delete**. If the deleted computers online again and scanned out by **Intrusion Detection Agent**, it will display in the Intrusion Detection windows again.

Chapter 11 Encrypted Disk (Endpoint Security Module)

By default, the type of all removable storages used in company is unclassified. System administrator can format non-encrypted disks into encrypted disks through the Removable-Storage windows. Encrypted disks only can be used in computers with agents installed; therefore, it blocks the virus from entering the LAN through removable storages.

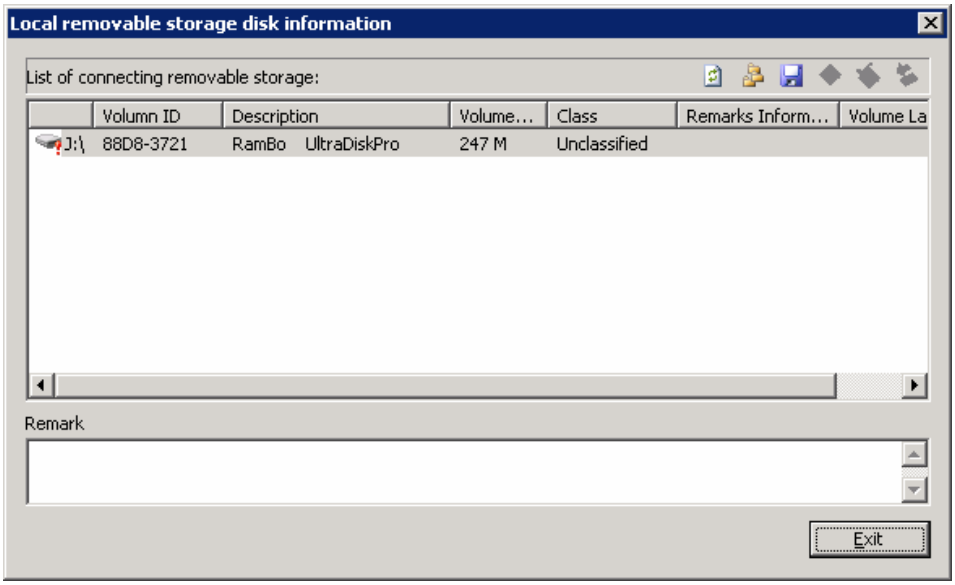
11.1 Disk Encryption

Firstly, plug in removable disks which are needed to be encrypted.

Secondly, go to **Tools** → **Classes Management** → **Removable-storage** to open the **Removable-storage Classes** windows.

Third, select **Operation** → **Local removable storage…** to open **Local removable storage disk information** windows to see the connecting devices information.

If the icon is  , it represents that the removable storage is not saved in the removable-storage database.



Refresh local removable storage disk information manually

Classify removable-storages. When a removable storage is plugged into computers with IP-guard agent installed at the first time, IP-guard will classify the removable storage into **Unclassified** class by default. Click this button to classify them into self-defined classes.

Click this button to confirm and save the removable-storage information. System administrator can classify disk, add notes, format and encrypt disk while saving.

Click this button to format and encrypt the selected disk. Once the selected disk is formatted and encrypted, all saved information will be deleted and the disk can only be used in those computers with agents installed.

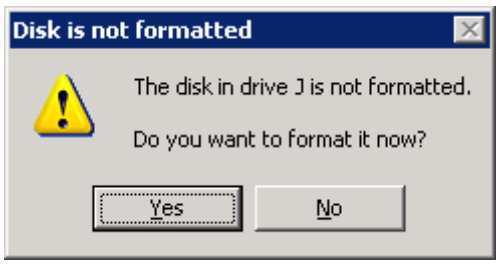
【Caution】

(1). Encryption function is only valid for users who registered IP-guard with register IDs. Otherwise, this button is gray and disable.

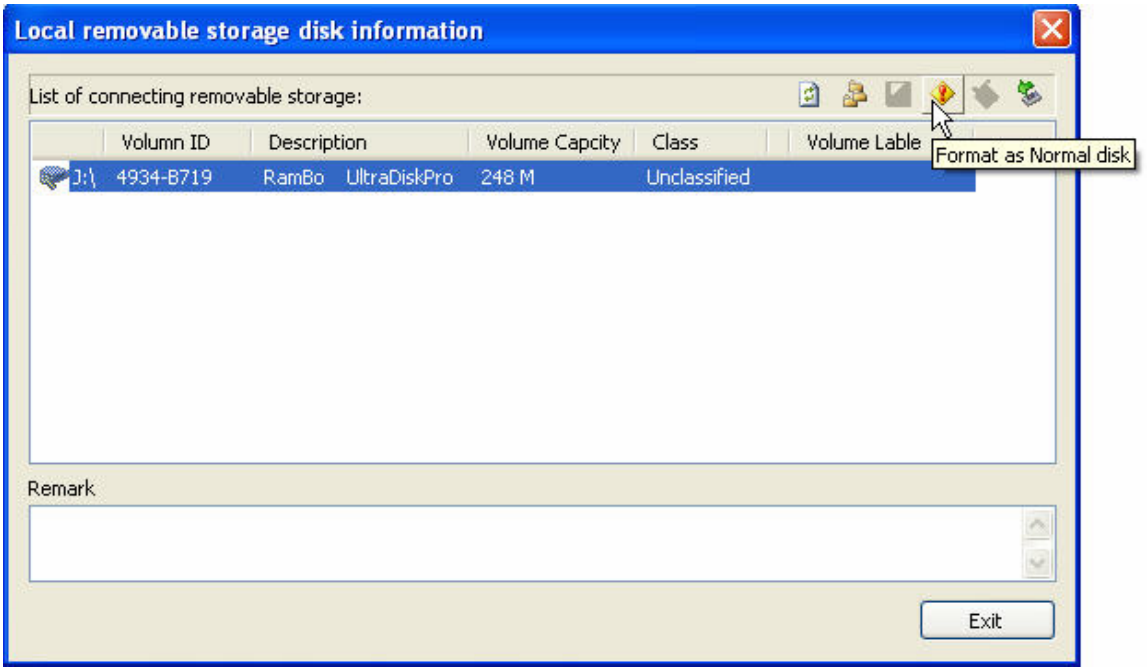
(2). If the disk is successfully encrypted, the icon will be . It represents that the operation is not saved. If saved, the icon will be .

11.2 Format Encrypted Disks into Non- encrypted Disks

1) Encrypted disks are only can be normally used in computers with IP-guard agents installed. When they are used in computers without agents installed, a dialogue box will pop up to prompt the user to format them. If **YES** is clicked, the user will format them into non-encrypted disks manually and the inside data will be completely deleted.



2) Plug in any encrypted disks, select **Operation → Local Removable-storage…** to open **Local removable storage disk information** window to see the connecting devices information. Administrator can format any encrypted disks into non-encrypted disks.



Select an encrypted disk, this button will light up. Click it to format the encrypted disk into a non-encrypted disk. Once succeed, the disk icon will be and its volume ID will be changed too.

For console computers, encrypted disks can be plugged out safely on the **Local removable storage disk information** windows of IP-guard console rather than on the System Tray of Windows.

For agent computers, **encrypted disks only can be safely plugged out** by this way: Go to **My Computer** and right click the encrypted disk to select **Eject device**.

11.3 Removable-storage Information

By default, there are two types of removable storage: **Encrypted Disk** and **Non-Encrypted Disk**. If the **Disk Type** is empty, it represent that this connecting device is non-encrypted.

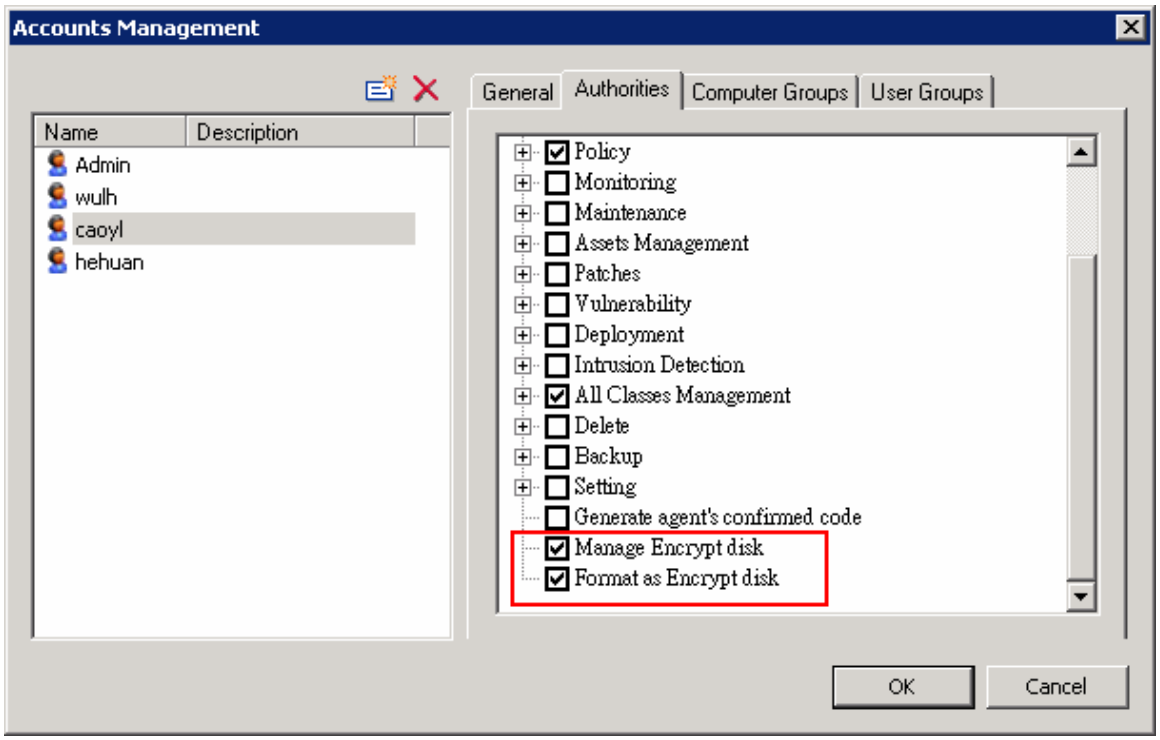
Volumn ID	Description	Remarks Information	Volume ...	Type	Partition Format	Volume Lable
8866-EC4E	SanDisk Cruzer		1904 M		FAT32	USB
4934-B719	RamBo UltraDiskPro		248 M	Encrypt disk	FAT	
4934-BD6D	SanDisk Cruzer		1904 M	Encrypt disk	FAT32	
142C-0503	SanDisk Cruzer		1904 M		FAT32	
344B-6F80	RamBo UltraDiskPro		247 M		FAT32	
4934-E5FE	RamBo UltraDiskPro		248 M	Encrypt disk	FAT	

11.3.1 Account Management

Select from menu bar, **Tools** → **Accounts(M)…**,;select an account on the left pane of **Accounts Management** interface, then select **Authorities** tab to view **Manage Encrypted disk** and **Format as Encrypt disk** options.

Manage Encrypt disk: Limit the operation rights on Managing Encrypt Disk, and it is used in class management.

Format as Encrypt disk: Format encrypted disks into non-encrypted disks or format non-encrypted disks into encrypted disks.



Admin account is a super administrator which has the highest rights to use all functions while other accounts do not have the permission to use these two functions unless they are granted.

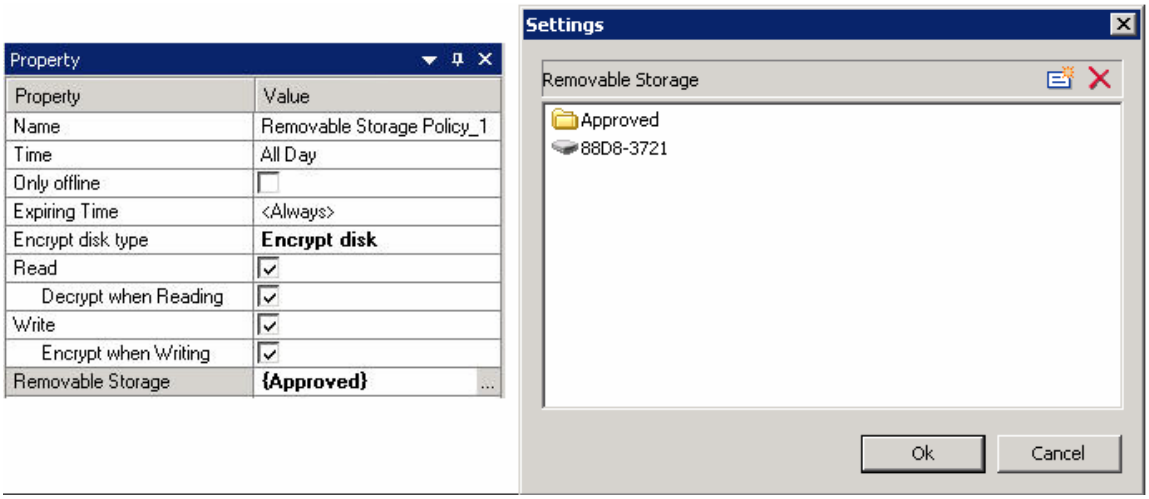
11.3.2 Removable-Storage Log

Select **Log** → **Removable-storage** to view the log of plug-in and plug-out actions of all removable storages in agent computers. If the **Disk Type** is empty that represents the removable storage type is non-encrypted disk.

Type	Time	Computer	User	Disk Type	Volumn ID	Description	Volume Lable
Plug In	2008-12-02 17:06:28	TECLINK-...	teclink		142C-0503	SanDisk Cruzer	
Plug In	2008-12-02 17:06:21	TECLINK-...	teclink	Encrypt disk	4934-E5FE	RamBo UltraDiskPro	
Plug ...	2008-12-02 15:46:35	TECLINK-...	teclink	Encrypt disk	4934-E5FE	RamBo UltraDiskPro	
Plug In	2008-12-02 15:46:06	TECLINK-...	teclink	Encrypt disk	4934-E5FE	RamBo UltraDiskPro	
Plug ...	2008-12-02 12:56:18	TECLINK-...	teclink		344B-6F80	RamBo UltraDiskPro	
Plug In	2008-12-02 12:56:13	TECLINK-...	teclink		344B-6F80	RamBo UltraDiskPro	

11.3.3 Removable-Storage Policy

System administrator can apply removable-storage policy to assign different rights to removable storages, as shown in the following illustration:



By Default, **Encrypted Disk Type** is **All** including two types: **Encrypted Disk** and **Non-encrypted Disk**. Select **Encrypted Disk** in the drop-down list box which indicates that this policy is only effective for encrypted disks.

System administrator can limit the operation authorities of specified removable storage by checking the checkboxes of **Read**, **Decrypt when Reading**, **Write**, and **Encrypt when Writing**. For details, please refer to **Removable-Storage Policy**. The use privilege of encrypted disks is the same as non-encrypted disks.

Chapter 12 Database Backup & Data Recovery

The difference between Main Backup in the following Section 11.1 and Data Backup in Section 11.2 are: The Main Backup (refer to Section 11.1) can be used to recover the IP-guard server in case of Database crashed or other accidents that caused the server cannot work properly or complete migration. **We strongly recommend to do complete full backup once after the server is in production stage since all computer and user groupings, classes management, policy settings etc. are settled.**

The meaning of Data Backup (refer to Section 11.2) is to backup the data such as screen snapshot history, document, mail, printing and key data. **We strongly recommend System administrator backup data regularly to prevent the hard disk storage getting full.** However, only backup data mentioned in Section 11.2 cannot help for server migration or recovery.

12.1 Database Backup

Backup Main Database

In order to prevent Database file crashed or other accidents that made the server cannot work properly, we strongly recommend System Administrator fully backup the database regularly.

[How to]

1. Stop the IP-guard server first (see Figure 11.1) and related services (OCULAR V3 SERVER and OCULAR V3 UPDATE) in System Services.

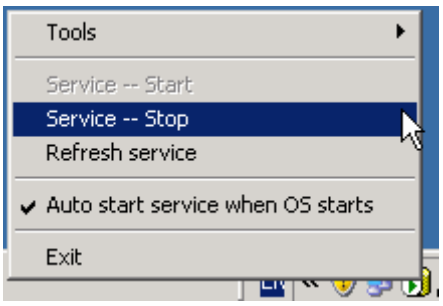


Figure 12.1 Stop IP-guard Server

2. Open **SQL Server Management Studio** and connect to the database

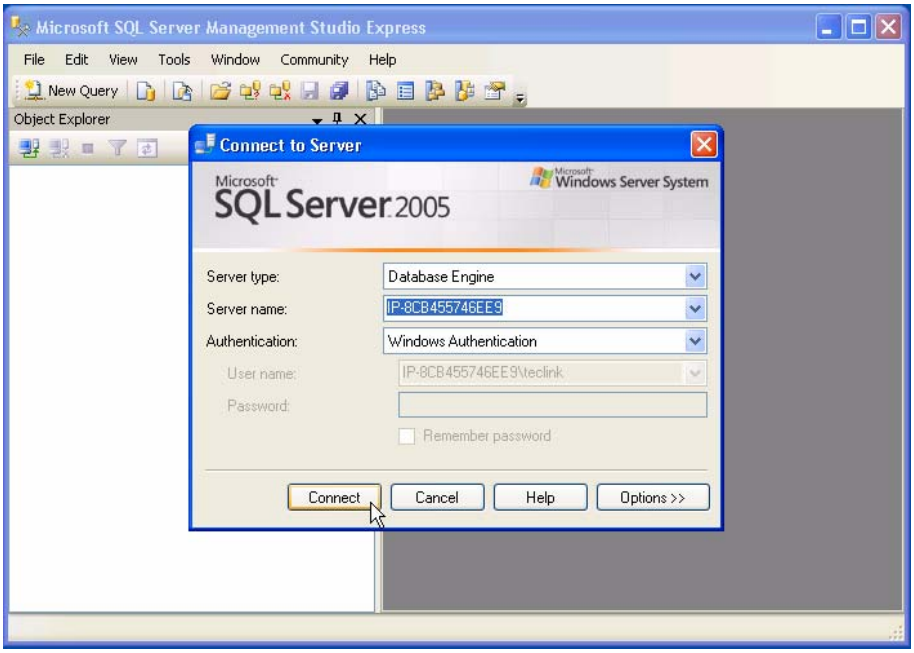


Figure 11.2 SQL Server Management Studio

3. In the **Object Explorer**, expend the **Databases**. You can see a Database called **OCULAR3**
4. Right click the Database **OCULAR3**, **Tasks → Back Up…** to backup the database (Figure 11.3)

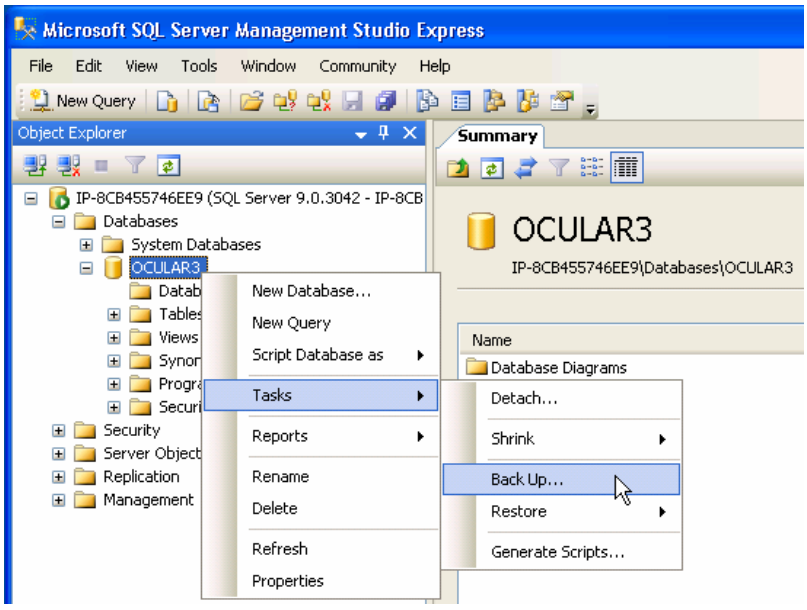


Figure 11.3 Detach Database OCULAR3

5. In the **Back Up Database – OCULAR3** window, add a **destination path** with **backup file name** e.g. IP-guard_full_backup.bak. Click the button **OK** to confirm (see Figure 11.4)

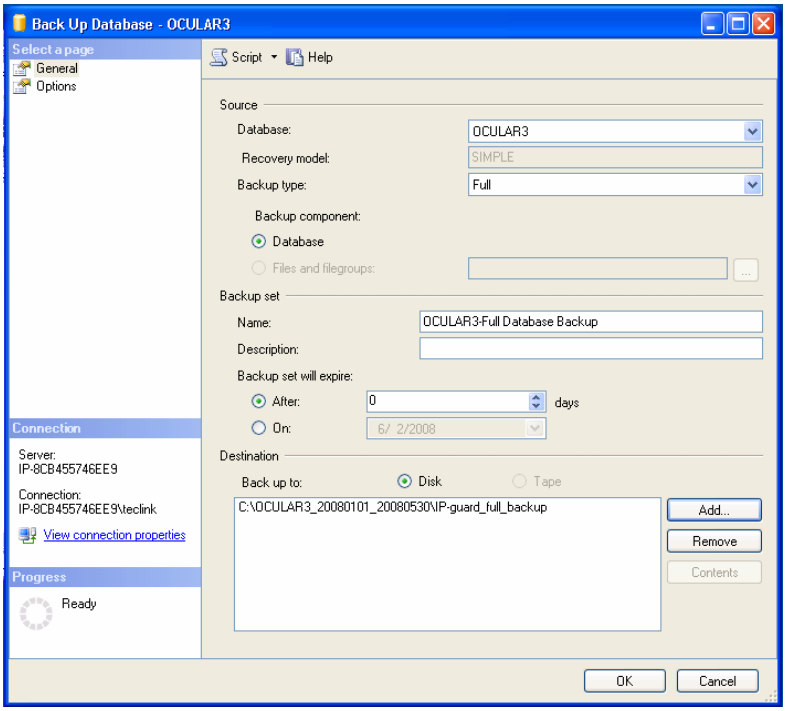


Figure 12.4 Backup Database

6. Click the button **OK** to complete the backup

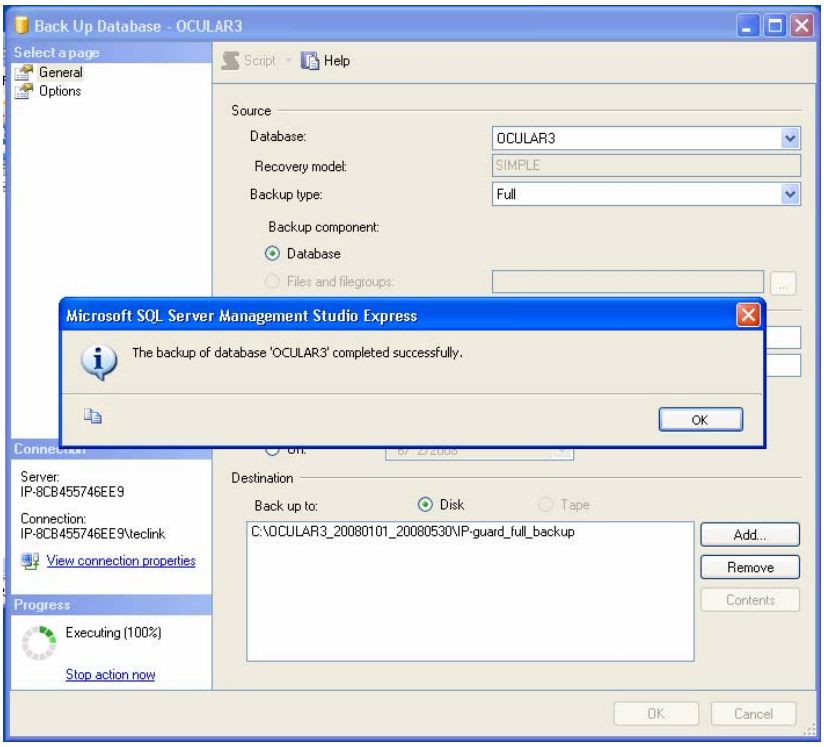


Figure 12.5 Complete Database Backup

7. Right click the Database **OCULAR3**, **Tasks → Detech…** to detach the database (see Figure 11.6)

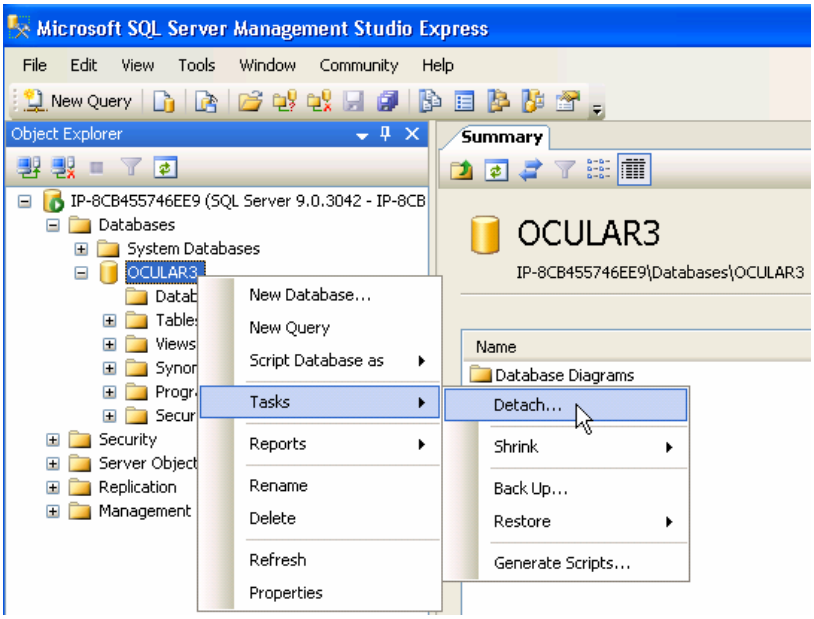


Figure 12.6 Detach Database

8. After detached successfully, System administrator can backup the following files and save into the backup folder:

File Extension	Files
***.MDF & *.NDF**	Backup all *.mdf and *.ndf files such as: OCULAR3_Data.mdf, OCULAR3_Log.LDF, OCULAR3_SCREEN_Data.NDF, OCULAR3_MAIL_Data.NDF, OCULAR3_DOC_Data.NDF
***.INI**	Backup all *.ini files such as: Update.ini, OServer3.ini, AssetQuery.ini
***.DAT**	Backup all *.dat files such as: Unins000.dat

Table 12.1 Backup Main Files

9. The database **OCULAR** has to be attached again after the backup completed in SQL Server Studio Management:

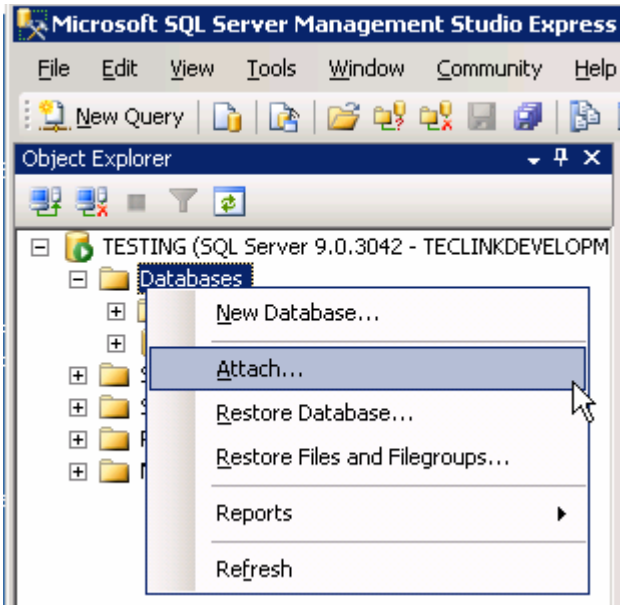


Figure 12.7 Attach Database

Backup Other Data

Another data such as screen snapshot, emails, and documents can backup easily. System administrators just need to copy those folders to desired backup storage device.

Figure 12.8 Backup Data Folders

12.2 Using IP-guard Console for Data Backup & Review

12.2.1 Data Backup

IP-guard Console provides a function for data backup, using this function can easily backup data to backup storage devices to prevent hard disk full.

[How to]

1. Select from **IP-guard Console → Tools → Data Backup and Review**
2. In the bottom part of **Data Backup and Review** Windows, click the button  to create a backup task (see Figure 11.9)

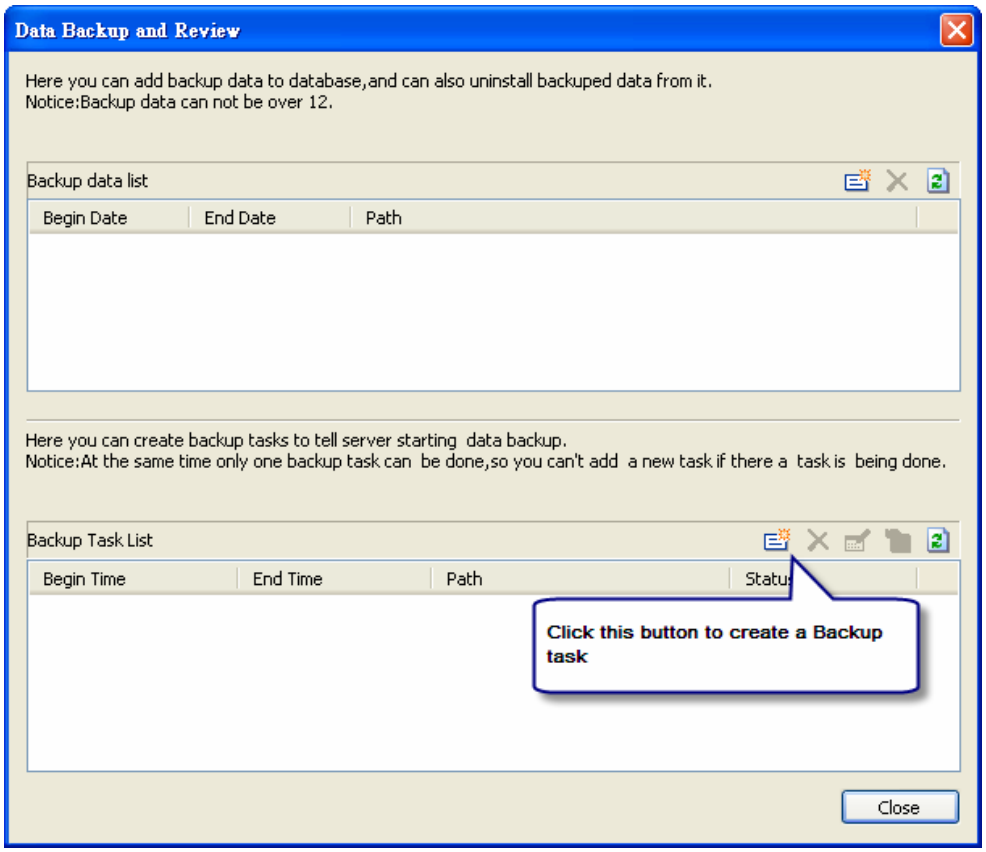


Figure 12.9 Create Backup Task

Other Operations in **Data Backup and Review** Windows:

 Stop the backup task.

 View the backup conditions such as data range, data backup options etc.

 View the details of backup process logs including startup/end status, progress log with corresponding success or failure reasons

 Refresh the Backup Task List

Table 12.2 Button Function for Data Backup and Review

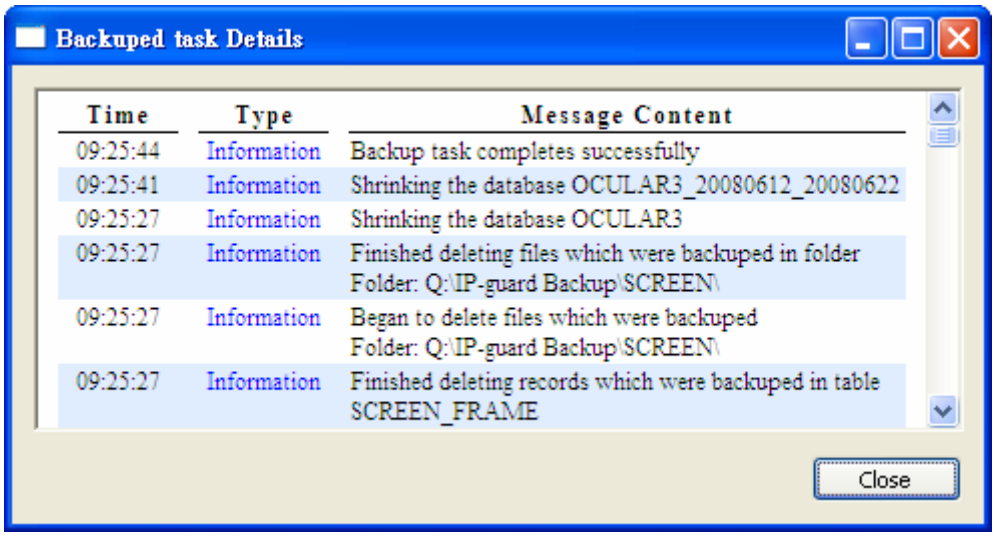


Figure 12.10 Backup Task Details

3. In the **Database Backup** windows, the following settings should be set:

   (a) select the required **date range** (start time and end time);

   (b) select the required **backup data** including major IP-guard key data (compulsory), document (optional), email (optional) and screen history (optional);

   (c) If the option **Delete the data after completion of the data backup** is selected, the files (document, email and screen history) saved in IP-guard server will be removed automatically. Otherwise, those data will remain at the IP-guard server root folder;

   (d) The size of the database will not be shrunk even after the data mentioned in (b) are backup. If required to release the space of database, you should select the option **Release the database space**, it may take longer time to complete the action. Otherwise, the database will not be shrunk automatically;

   (e) Select the **backup path**;

   (f) Click the button **OK** to confirm

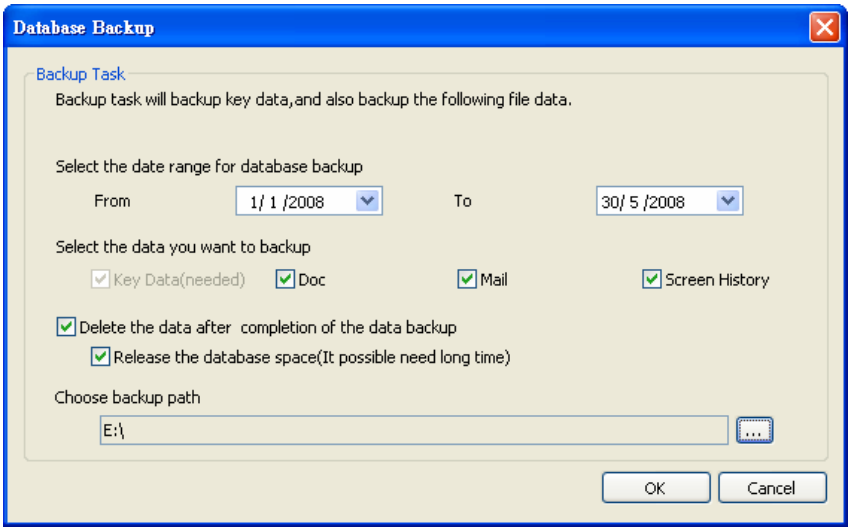


Figure 12.11 Backup Task

4. In the **Backup Task List**, the status of backup process showed in the list. The status is Success, Failed or Cancelled. Double click the task to see the detailed logs.

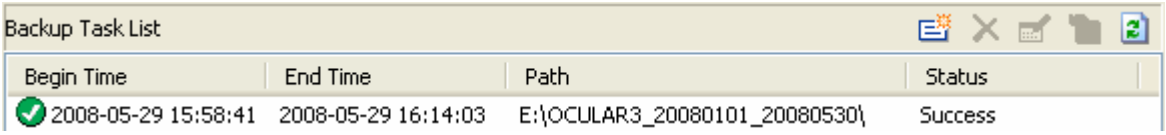


Figure 12.12 Backup status

[Important]

About Backup...
Only one task is allowed processing at a time. If the backup is processing, it is not allowed adding any other tasks. Also, only the most recent 10 tasks showed on the list.

12.2.2 Review Backup Data

To review the backup data, System Administrator easily adds the backup data folder back to IP-guard console. Notes that loading the backup data is only to restore backup data to the server, it does not undermine the existing data.

[How to]

1. Select from **IP-guard Console → Tools → Data Backup and Review**
2. In the upper part of the **Data Backup and Review** Windows, the added data tasks are listed (see Figure 11.13)

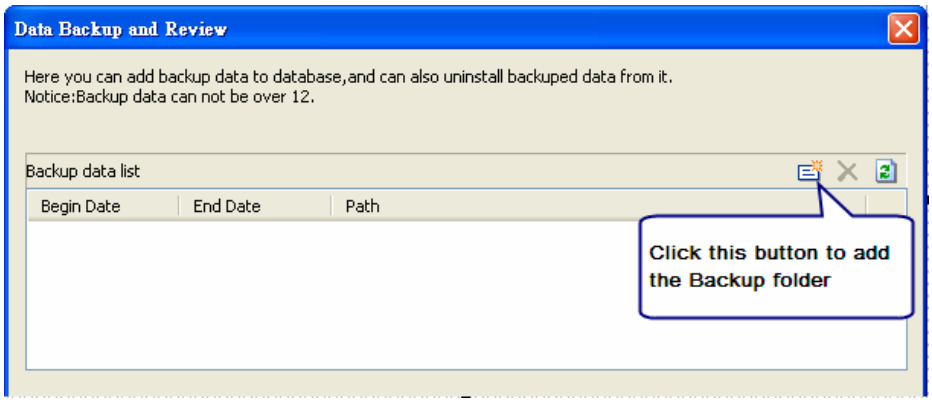


Figure 12.13 Add and Review Backup data

- **Add the Backup Data**

  (a) Click the button to add the backup data

  (b) In the **Browse** Windows, select the directory stored the backup data file

  (c) Click **OK** to confirm to add the data

  Note that the added data can be viewed and queried from Console directly. Also, the maximum number of added data task lists is 12 only.

- **Remove the Backup Data**

  (a) Select the added data item and click the button to remove it

  Note that once the data is removed from the list, it cannot be viewed and queried from the Console anymore until added again.

Chapter 13 Tools

13.1 Account Management

Admin account is a super administrator which has the highest rights to use all functions. Using **admin** login account can create other user accounts to access IP-guard with different access rights.

Select from menu bar, **Tools→Accounts**, System administrator can view the existing users or create new users.

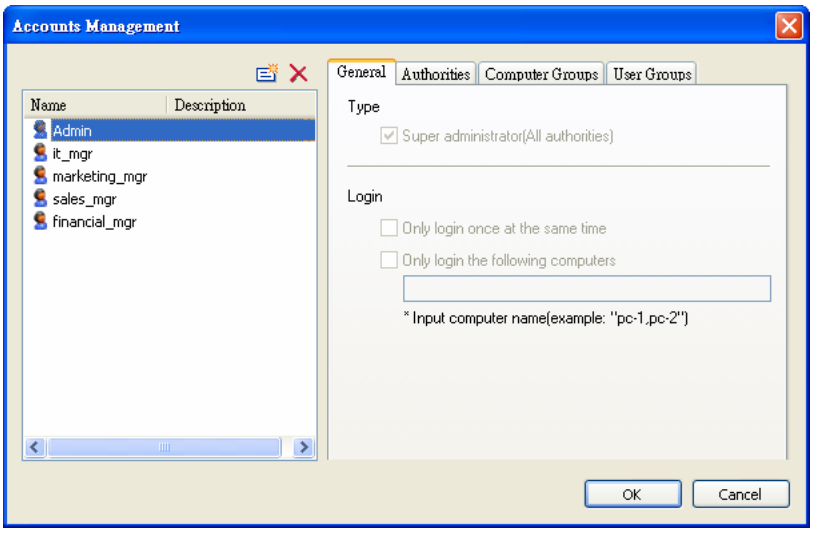


Figure 13.1 Account Management

Create user account, also can input the Description

Delete user account. Notes that **Admin** account cannot be deleted

Accounts Management has 4 settings including **General**, **Authorities**, **Computer Groups** and **User Groups**

General	Specify the type of account and login mode
Authorities	Specify the functions access rights of the account, please read the following table for details.
Computer Groups/User Groups	- Either to limit the management range in Computer Groups or User Groups. - if Computer Group is selected, User Group cannot be selected or vice versa - If Computer Groups is set to All, User Group is also set to All by default

Functions Access Rights:

File	Limit the operation rights on Computer tree or User tree such as create, move, rename or delete computers / users. Also, limit the print and export functions
Control	Limit the agent control rights including Lock/Unlock, Notify, Log off, Power Down/Restart, Remote or Uninstall agents
Statistic	Limit the statistics log enquiries and access rights including Application Statistics, Web Statistics and Traffic Statistics etc.
Log	Limit the event log enquiries and access rights including Basic Event logs, Window Change Logs, Application Logs, Web Logs, Document Logs, Shared File Logs, Printing Logs, Asset Changes Logs, Policy Logs, System Logs, Backup Logs and Removable-storage Operation Log
Policy	Limit the policies enquiries and modification including Basic Policy, Application Policy, Web Policy, Device Policy, Printing Policy, Screen Snapshot Policy, Logging Policy, Remote Control Policy, Network Policy, Traffic Policy, Mail Policy, IM File Policy, Document Policy, Alert Policy and Removable-Storage Policy
Monitoring	Limit the monitoring enquiries and control rights including Real-time Screen Snapshot, View Screen History, Export Screen Snapshot, Instant Messages and Mail
Maintenance	Limit the operation rights on remote maintenance such as view remote information, remote operation, remote control and remote file transfer etc.
Assets Management	Limit the operation rights on Assets management including Query, Define Asset and Edit Asset
Patches	Limit the operation rights on Patches including Query, Parameter Setting and Executing
Vulnerability	Limit the operation rights on Vulnerability including Query and Parameter Setting
Deployment	Limit the operation rights on Deployment including Package Query, Package Setting, Task Query, Task Setting and Tasking Executing
Intrusion Detection	Limit the operation rights on Intrusion Detection including View intrusion detection, Set Intrusion Detection and Set Policy

Class	Limit the operation rights on Classes management including Application Class, Website Class, Time Type, Network IP Class, Network Port Class and Removable-storage Class
Delete	Limit the operation rights on Delete including Delete Logs, Delete Instant Messages and Delete Mails
Backup	Limit the operation rights on Backup including Backup Logs and Review
Setting	Limit the operation rights on Setting including Agent Search Range and Set exclude range of the agent
Generate agent's confirmed code	Limit the operation rights on Generating agent's confirmed code. Our recommendation is this right should not assigned to other users which are not IP-guard System Administrator
Manage Encrypt Disk	Limit the operation rights on Managing Encrypt Disk
Format as Encrypt Disk	Limit the operation rights on Formatting Encrypt Disk

Table 13.1 Account Management

13.2 Computer Management

To facilitate System administrator to mange installed agents and query the licenses information easily, System administrator can use the Computer Management Console (**Tools → Computers**) to check out the information. The list contains the following information: Name, Computer, Agent ID, IP Address, MAC Address, Group of Agent, First Appeared Time, Last Appeared Time, Agent Installed Version Number and Agent Installation Date

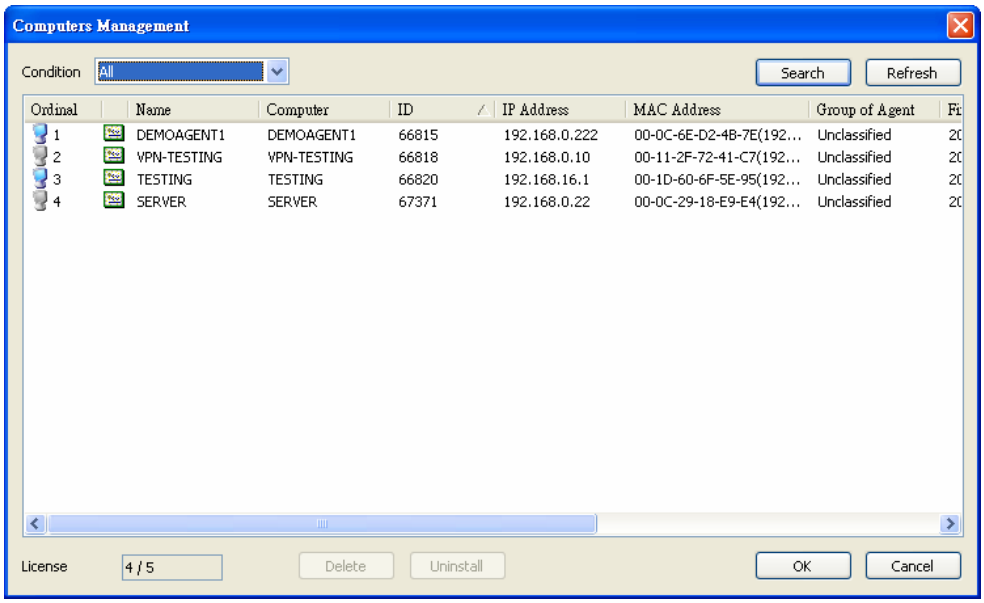


Figure 13.2 Computers Management

List of Computer Information:

	Represents a license is granted to the agent. If this icon not appears in the highlighted agent, it means that it is over the licenses range. No more available license can be granted to that agent.
Name	The name of agent displayed in the Console
Computer	The computer name of agent
ID	Agent ID generated by IP-guard
IP Address	Agent's IP address
MAC Address	Agent's MAC address
Group of Agent	Agent's belonging group
First Appeared	The first appeared time of the agent
Last Appeared	The last appeared time of the agent
Version	Agent's current installed version
Install Date	Agent's installation date

Table 13.2 Computer Management – List of Computer Information

Searching Conditions:

All	By default, all agents are listed
By IP address	Search by specifying the IP range
By First Appeared	Search by specifying the first appeared time range
By Last Appeared	Search by specifying the last appeared time range
By Agent ID	Search by specifying agent ID
By Name	Search by specifying computer name, support wildcard input

Table 13.3 Computers Management – Searching Conditions

Operations:

Delete	This option includes two actions: uninstall agent automatically and release the agent license. The agent will not appear in the computer tree.
Uninstall	To uninstall agent, not include releasing the license. The agent still appears in the computer tree.

Table 13.4 Computers Management - Operations

After the above action is selected, click **OK** to confirm the action. Otherwise, if only **Delete** or **Uninstall** button is clicked, no actual actions take effective unless to click **OK** button to confirm.

13.3 Alert Message

Select from **Tools→Alert**, all real-time invoked policies alert messages are logged in the popup windows. If **popup alert bubble** is checked in **Tools→Options**, when some agents invoked some policies, the alert bubble will popup in the right-bottom corner, click the alert bubble to see the details of alert message.

In the alert message windows, the maximum display records are 500, this setting can be set from **Tools→Options→Console Settings→Alert→Alert Dialog** to change the maximum display records.

Notice that when Console is closed or re-login, these messages will be clear. To review the history, go to **Log→Policy Logs**.

13.4 Classes Management

System administrator can set different classes including Application Class, Web Class, Removable-storage Class, Time Type Class, Network IP Address Class and Network IP Port Class to facilitate the query, statistics and policy settings

13.4.1 Application Class

Go to **Tools→Classes Management→Applications** to open the Application Classes windows. By default, there are two classes there: Unclassified and Windows Application

Unclassified	All application programs are collected from agents, the program is classified into **Unclassified** when it is first scanned. System administrator can create other classes and using drag and drop method to move the program located in **Unclassified**.
Windows Application	Includes Windows system related applications

Table 13.5 Application Classes Management – Default Classes

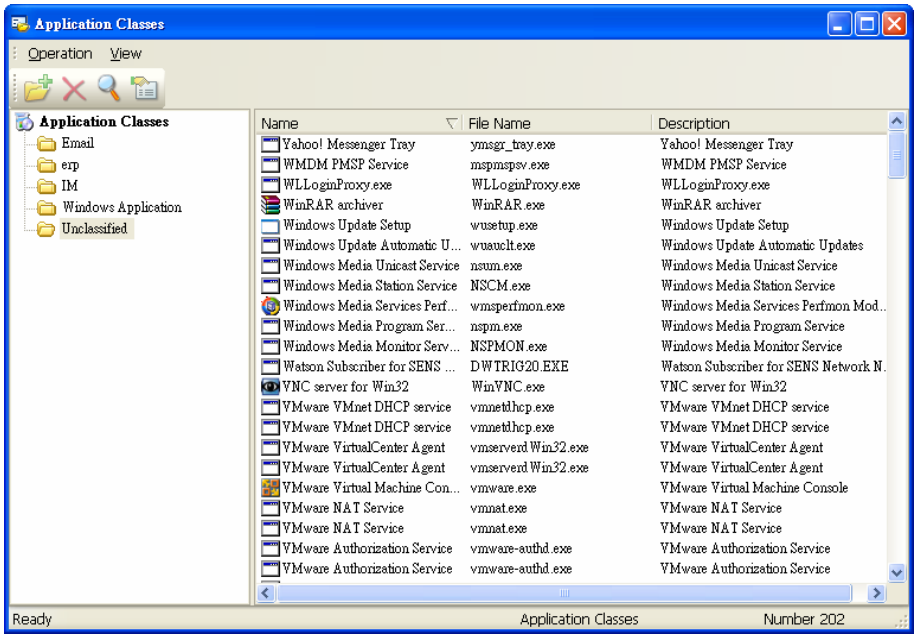


Figure 13.3 Application Classes

System administrator can create different classes and classified the applications from **Unclassified** into customized classes.

New	Select **Operation→New** or under the **Application Classes** tree right click to **New** a class. Sub-class can be created under a class
Move to	Select **Operation→Move to…** or using **drag and drop** method to move the application from **Unclassified** to specified customized class. Press Ctrl button for multiple selections
Search	Select **Operation→Search** can search specified application programs and class location. Input by application name, file name or descriptions.

Table 13.6 Application Classes Management – Operations

Caution:

About Unclassified and Windows Applications classes
Unclassified and Windows Applications classes cannot be deleted and create sub-classes.

13.4.2 Web Class

Go to **Tools→Classes Management→Websites** to open the Website Classes windows. By default, no class is created, System administrator required to create classes and identity manually. The websites identity supports wildcard input

New Website Class	Select **Operation→New→Website Class** and rename the class. Can create sub-classes under a main class
New Website Identity	Select Operation→New→Website Identity and input the name and website address. The website address can be complete URL or wildcard input e.g. *sina*, *mail*, *game* etc.
Search	Select Operation→Search or click the button to search the specified website belonging to which classes or determine the website address or classes exist or not

Table 13.7 Website Classes Management

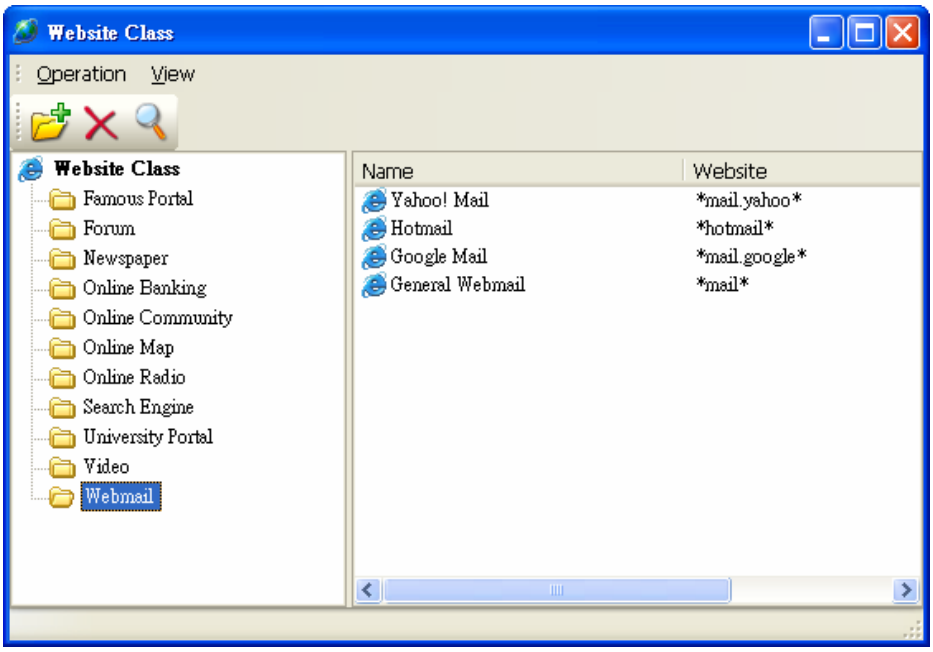


Figure 13.4 Website Classes

13.4.3 Removable-storage Class

Go to **Tools→Classes Management→Removable-storage** to open the Removable-storage Classes windows. By default, there is a class called Unclassified, System administrator required to create classes manually.

There are two methods to gather the Removable-storage information:

1. From Agent	All removable-storages used by agent computers, all information is collected and placed in **Unclassified** class, System administrator can move them to another self-defined classes
2. From Console	System administrator can plug-in any removable storages to a computer which installed with Console. Select Operation→Local Removable-storage… or click a the button  to open Local removable storage disk information windows to see the connecting devices information. If the icon is  , it represents that that removable storage still not saved in the removable-storage database  Set the removable-storage class, click this button to classify the connecting storage to self-defined class. Notes that adding **remarks** information to facilitate System administrator to review and identify the storage.  Click this button to confirm and save the removable-storage information.

Table 13.8 Removable-storage Classes Management

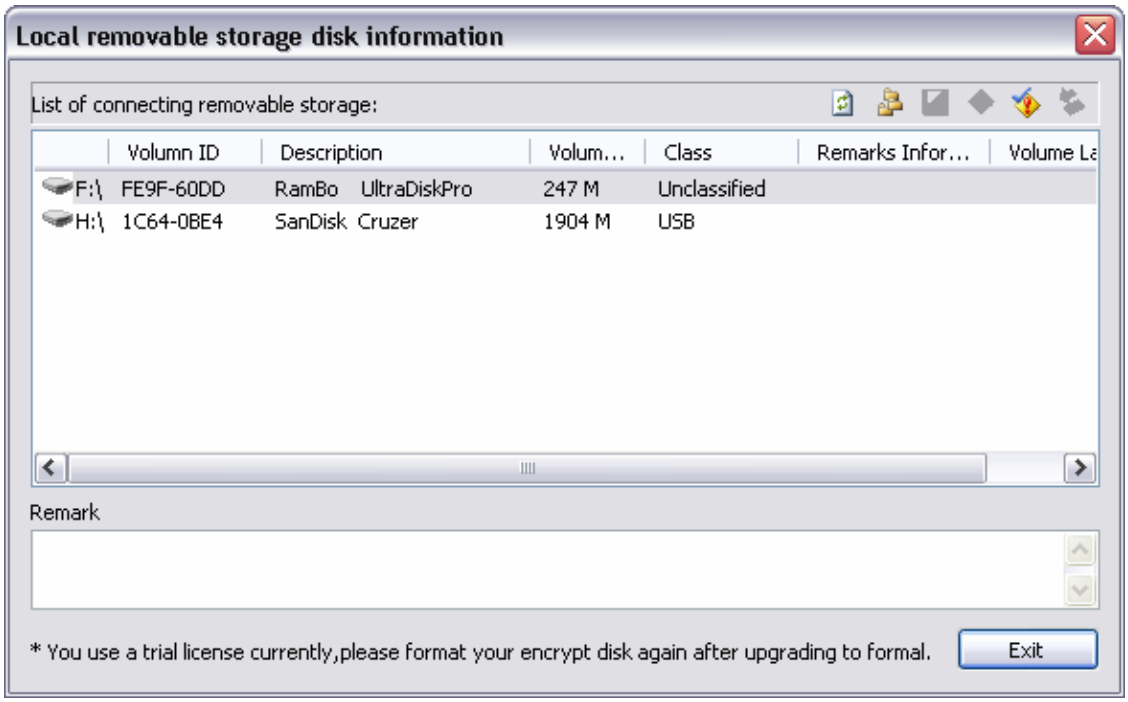


Figure 13.5 Removable storage Management

13.4.4 Time Types Class

To facilitate searching and analyzing, System administrator can self-define the time range. Select **Tools→Classes Management→Time Type**, System administrator can view the existing time type. By default, there are 4 types: All Day, Working time, Rest and Weekend.

System administrator can custom the existing time classes except All Day class or create new classes as required.

	Add time type, click this button and input the name and select the time range manually. By default, it is set to All Day
	Delete time type, select the time type class and click this button to delete the class. The default four classes cannot be deleted.

Table 13.9 Time Type Classes Management

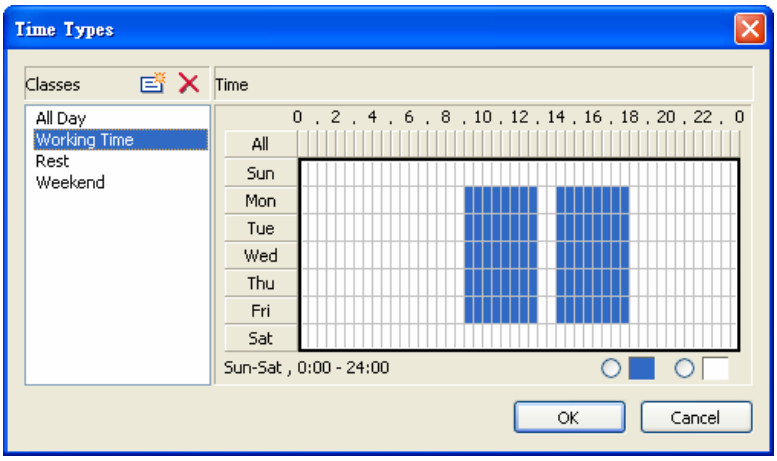


Figure 13.6 Time Type Classes

13.4.5 Network IP Address Class

Select **Tools→Classes Management→Network Address**, System administrator can define the network address classes. By default, there are five classes: All, LAN, Outer, Intranet and Internet. As LAN and Outer classes cannot be amended, they are hidden in the Network IP Address Class management.

When input the Intranet network IP address range, system automatically generates Internet IP address range i.e. out of the Intranet range belongs to Internet network range. Except the default classes, System administrator can add new classes and input the target range

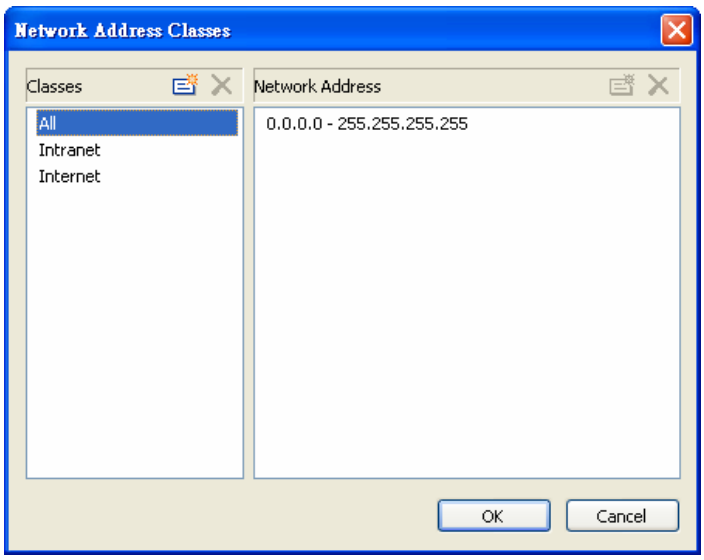


Figure 13.7 Network Address Classes

Caution:

About Network IP Address Class
In the Network IP address class, the LAN and Outer classes are hidden, but they are visible in statistics and event log searching. Actually, Intranet is LAN while Outer is Internet. Once the LAN address range is defined, the range of other classes can be confirmed

13.4.6 Network IP Port Class

Select **Tools→Classes Management→Network Ports**, System administrator can define the ports. By default, there are seven classes: All, ICMP, TCP, UDP, Mail, Web and Network Share. The classes All, ICMP, TCP and UDP cannot be added or amended their settings while others can add and amend.

Except the default classes, System administrator can create port classes and input the target control ports manually. All defaults port settings cannot be deleted or renamed, however, the manual added classes can be deleted or renamed.

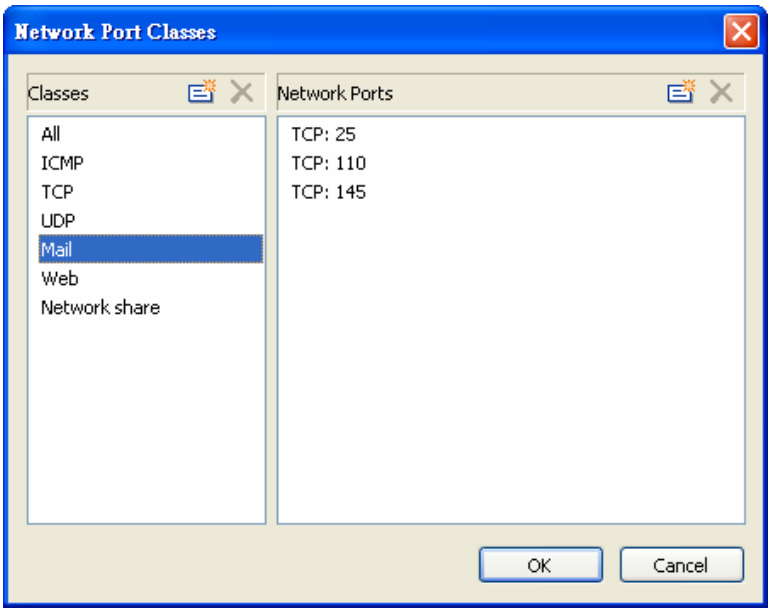


Figure 13.8 Network Port Classes

13.5 Server Management

Select **Tools→Server Management**, System administrator can check the server information using Console including: Basic Information, Database file, Directory and Disk Space.

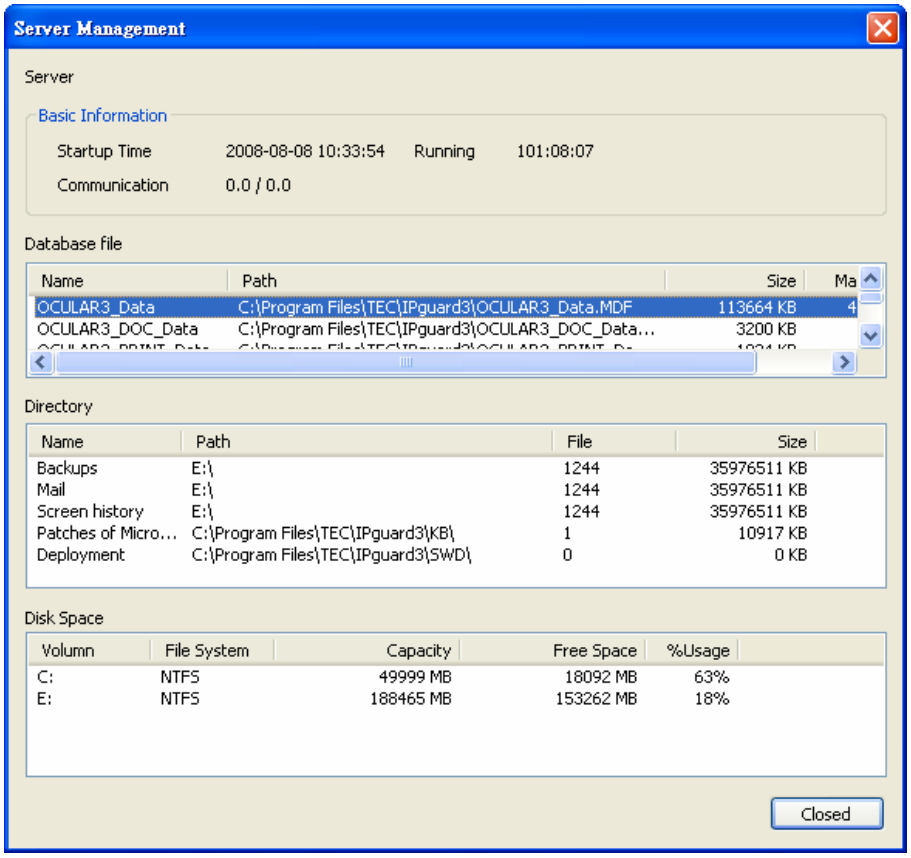


Figure 13.9 Server Management

Basic Information		Includes server startup time, running time and real-time bandwidth
	Startup Time	The time of server startup time
	Running	The total running time after server startup
	Communication	The real-time bandwidth flow (send / receive) between server and agent in KB
Database File		The name , path, size and maximum capacity of Database file
Directory		Includes Backup, Mail, Screen history, Patches and Deployment folders information (name, path, number of files and file size)
Disk Space		Server disk space information including volume, type of file system, capacity, free space and percentage usage.

Table 13.10 Server Management

13.6 Agent Tools

13.6.1 Confirm-code Generator

In case of any emergency while the agent cannot communicate with server (scenario: no Internet connection), some strict policies such as cannot decrypt presentation PowerPoint or prohibit using USB devices are still running. In this case, how the System administrator help to release policies or uninstall agent from the client computer is using Confirm-code generator. The followings are the procedures to release all policies or uninstall agent under approval.

1. Ask the agent user to press **Ctrl** + **Alt** + **Shift** and then press **ocularat** to open the agent tool.

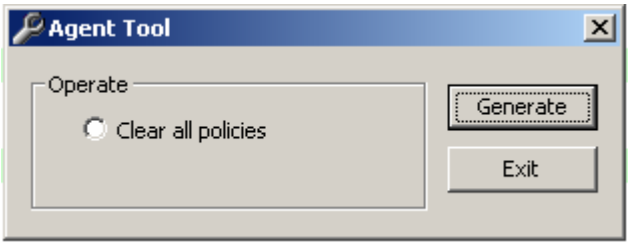


Figure 13.10 Agent Tool

2. Select **Clear all policies** and then click the **Generate** button
3. a window **Check confirm code** will popup, the agent user is required to report the **Operate Code** to System administrator

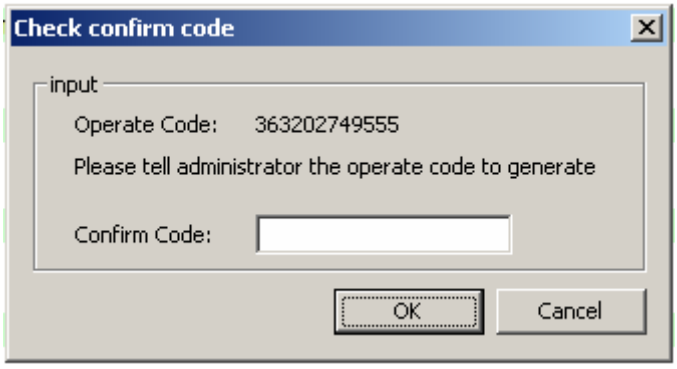


Figure 13.11 Check confirm code

4. System administrator is required to login Console, select **Tools→Agent Tool→Confirm-code generator** to input the **operate code** reported from agent user and click Parse button to analyse the agent information

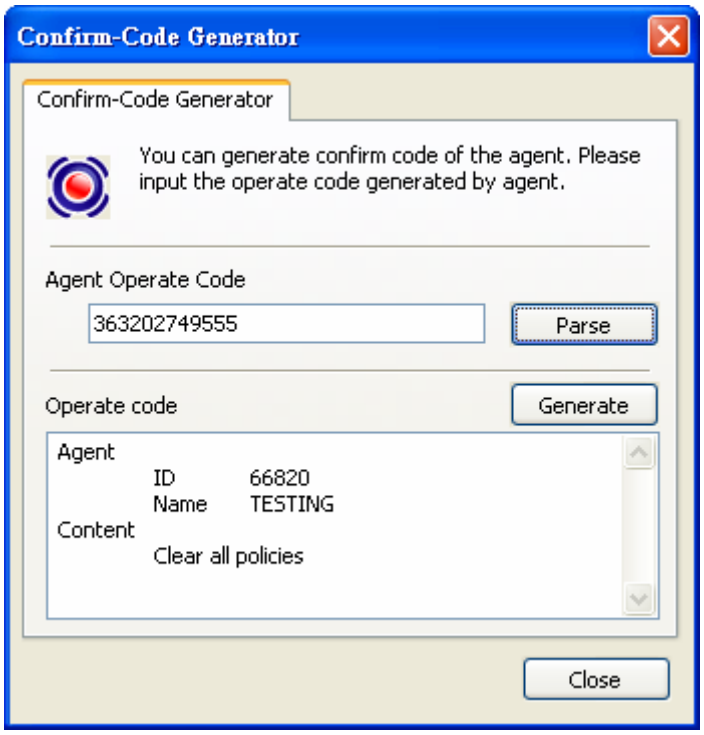


Figure 13.12 Confirm-Code Generator

5. System administrator is required to click Generate button to get the code generated by system

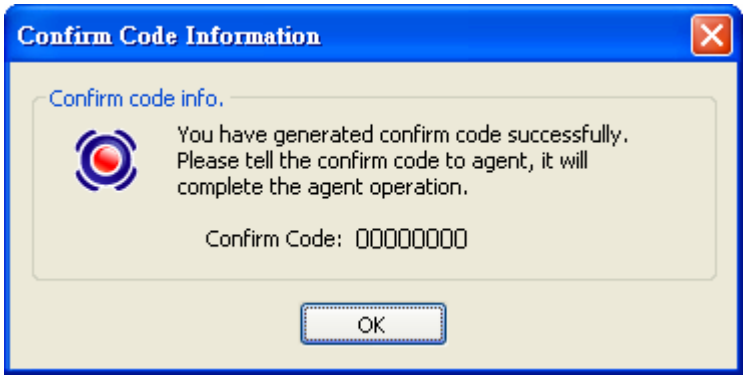


Figure 13.13 Confirm Code Information

6. System administrator tells the generated confirm code to agent user and ask him/her to input the confirm code
7. Agent user clicks **OK** to confirm

The normal way to uninstall agent please refer to Section 2.6.2 Uninstall Agent

13.7 Options

Select **Tools→Options**, System administrator can check or amend existing Console and Server settings. The following tables show all default values

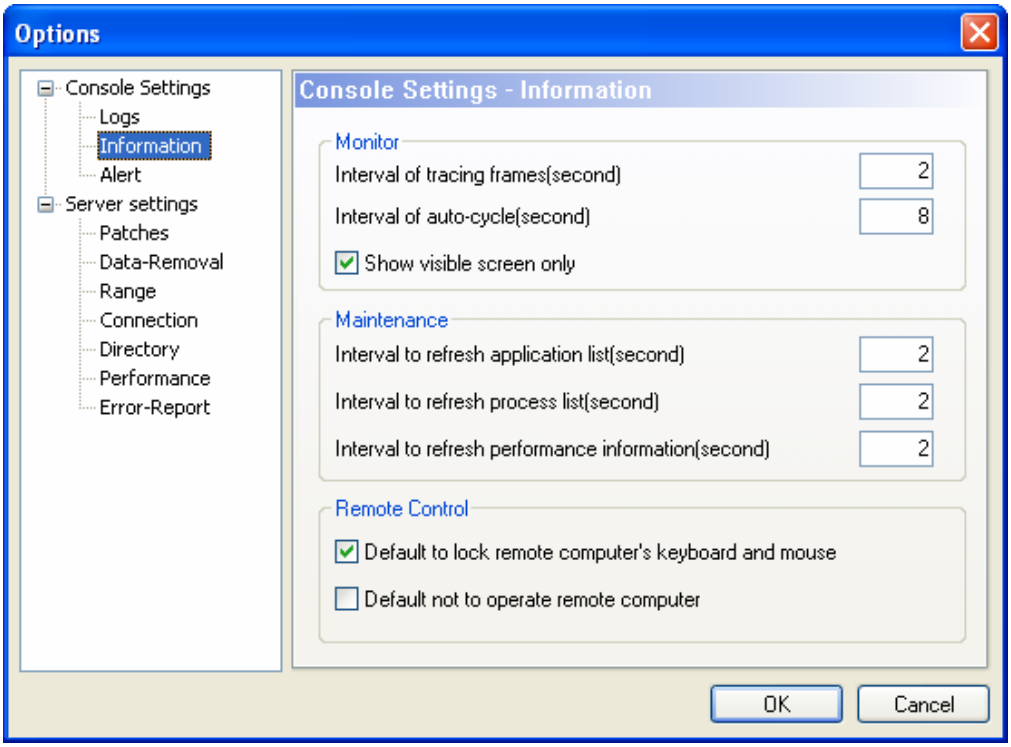


Figure 13.8 Server Options

13.7.1 Console Settings

Log		
	Search logs	the **max records show in logs on each page** is set to **20**
	Quick Settings	Option for user to **quit** console program or minimize **windows to system tray area**
Information		
	Monitor	the **interval of tracing frames (seconds)** is set to **2** the **interval of auto-cycle (seconds)** is set to **8**
	Maintenance	- the **interval to refresh application list (seconds)** is set to **2** - the **interval to refresh process list (seconds)** is set to **2** - the **interval to refresh performance information (seconds)** is set to **2**
Remote control		-Default to lock remote computer's keyboard and mouse -Default not to operate remote computer
Alert		
	Alert Dialog	**the max number (item) of showing logs in alert dialog** is **500**
	Settings	- the option **popup alert bubble** is **checked** and **the lowest alert level of**

		popup bubble is set to **Low** - if this option is enabled, real-time alert bubbles are popped up in the Console when policies invoked

Table 13.11 Options – Console Settings

13.7.2 Server Settings

Patch		
	Default Settings	**1. Install patches on new agents automatically** - If this option is checked, all new agents will install all downloaded patches. Otherwise, no patches will be installed on new agents - default is **unchecked** **2. Download new patch automatically** - If this option is checked, all new scanned patches will be downloaded automatically. Otherwise, the new scanned patched will not be downloaded - default is **unchecked**
Data-Removal		- If any items are checked and input the Days for keeping (range: 5 – 180 days), the data will only keep the latest specified days, the older data which is out of the specified days will be deleted automatically - the data types include: Basic Event logs, Document Operations Logs, Web Logs, Application Logs, Assets Change Logs, Printing Logs, Policy Logs, System Logs, Shared Files Logs, Removable Storage Operation logs, Screen History, Instant Message, Mail, Application Statistics, Web Statistics and Traffic Statistics - default is **all unchecked** which means no data will be deleted automatically
Range		**1. Search Range** - The following two cases may cause agents cannot communicate with server and/or not appearing in the network tree: • Not specified server IP address when packing agent • Change of server IP address In these cases, the search ranges should be set - To make the input search range to become effective, the option **Apply Active Polling** must be **checked** too in **Server Settings→ Connection**. Otherwise, the search range input is not effective - When target agents are found and appear in the network tree properly, the search range can be removed. **2. Exclude Range**

	- All agents in the specified exclude ranges cannot communicate with server. If the agent currently is communicating with server, once the exclude range is applied, the agent will become grey color after 3 minutes. - Notes that all applied policies are still effective for excluded agents - **Restart server** is required after input the exclude range to make it effective No range is set by default.
Connection	**1. Bandwidth settings between server and agent** - the range is limited from 1 to 102400kb/s - If server is in LAN environment, this setting is not required. However, it may apply in VPN environment **2. Active Polling** - By default, this option is **checked** because it prevents some agents do not know server IP address and cannot communicate with server normally, make sure this option is enable. - When no search range is set in **Search Range** and this option is checked, it means server will only scan local network - When search range is set and this option is checked, it means server will scan local network and also the specified input search range. - if this option is not enable, some agents may never communicate with server as they are missing server information
Directory	By default, all directories are located under IP-guard installation path. System administrator can change the patches and backup paths including: deployment, Backup email, Screen history, Document Backup and Microsoft Product Patches. Any directory paths changed, the data will not automatically move to new directory. IP-guard server must be stopped and then move the data to new directory as required. **Restart server** is required after changing any paths.  Select target object and then click this button to open the Directory Settings, select the new path. Click OK button to save the setting. The new path setting becomes effective after server restarted.  Click this button to restore to default directory settings. The restore

	path setting becomes effective after server restarted.
Performance	**1. Fixed Mode** **-** if this option is selected, it means the number of agents is specified handled by server - The range is available from 0 to 100. **2. Dynamic Mode** - This option is selected by default - if Normal is selected, it represents the average usage rate of sqlserver used by oserver3 is 30%. If High is selected, the upper limit is 50% while if Low is selected, the upper limit is 10% - Generally speaking, the higher performance of the server under dynamic mode, the higher number of agents that can be handled by server - For some real-time operations such as monitor the real-time screen snapshot or remote control, these are not affected by this option.
Error-Report	- the agent verification error messages will only be logged when this option is enable and can be found in **Event Log → System Logs**. - The details description of report levels are as following: **All**: Report all errors **Low**: the results returned from agent are not expected by server **Moderate**: over license **Important**: Serial number or checkcode error **Critical**: Communication between agent and server corrupted caused by exclude range is set

Table 13.12 Options – Server Settings

Chapter 14 Audit Console

14.1 Logon to Audit Console

Audit Console major audits all IP-guard Console System Administrators/Users and logs all operations done by them in the Console such as Account Login/Logoff; when they create/modify/delete policies etc. operations. The Audit administrator can easily view that information in the Audit Console.

[How to]

1. Open the IP-guard Console from **Start → All Programs → IP-guard V3 → IP-guard V3 Console**

2. Logon into audit console using **audit** as logon name. By default, the password is blank.

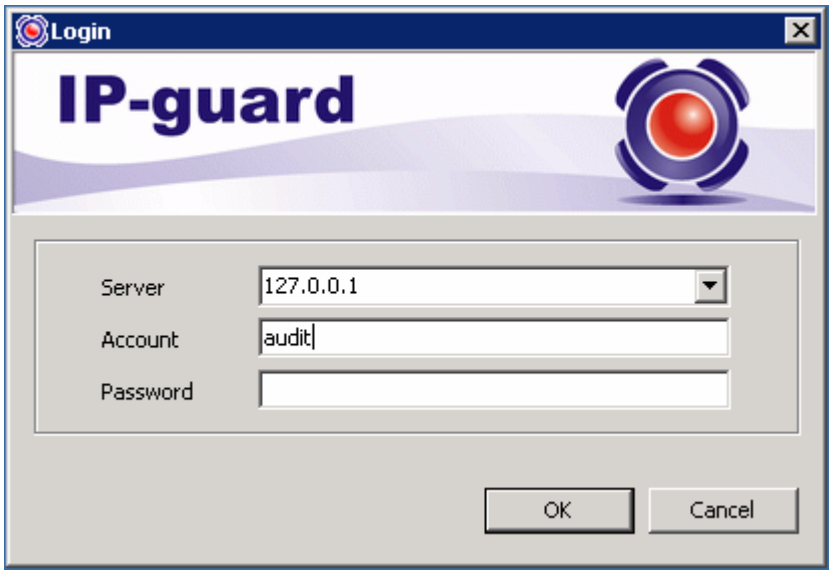


Figure 14.1 Login Audit Console

14.2 Audit Console Interface

Audit console includes: the title bar, menu bar, the Toolbar, the administrator column, the data panel, searching panel and the status bar.

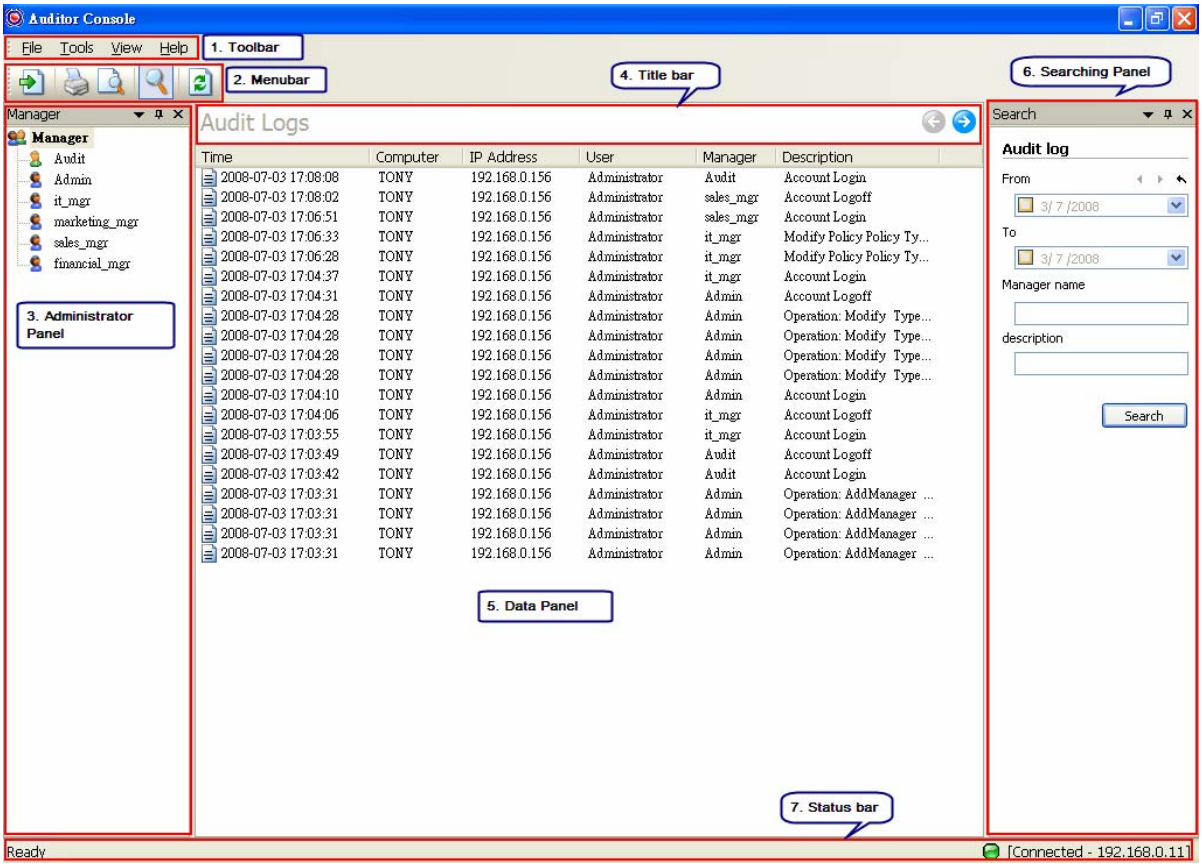


Figure 14.2 Audit Console Interface

The administrator panel lists all administrators and IP-guard Console users, the corresponding operation logs displayed in the data panel once the user selected from the administrator panel.

IP-guard Audit Console provides print and export functions to reserve the useful logs, also provide delete function to delete the audit data

[Functions]

Print / Print Preview	Select from **File → Print / Print Preview** to print the current log page
Export	Select from **File → Export** to export the audit log or right click from the Data Panel to select **Export →** 1) **Records of Current Pages** 2) **All Matched Records**
Delete	Select from File → Delete to delete the audit log or right click from the Data Panel to select **Delete →** 1) **Selected Records** 2) **Records of Current Page** or 3) **All Matched Records**

Table 14.1 Audit Console Common Functions

14.3 Using Audit Console

Audit Log

Time	Recorded time for corresponding operation
Computer	Logon Computer Name
IP Address	Logon Computer IP Address
Manager	Administrator Account Name
Description	Descriptions of the operations done in IP-guard Console by Administrator

Table 14.2 Audit Log

Audit Query

Date Range For the designated date range, the default start time and end time are not clicked, that is, all log data are searched and display as results. To specify the date range, click the start time and end time:

Icon	Descriptions
	Select the date as the start time from the calendar
	Select the date as the end time from the calendar
	Restore to default setting

Manager Name Search with specified administrator

Description According to the description of the audit log information to query specified logs

Table 14.3 Audit Query

Technical Support

Thank you for choosing our product. It is our commitment to provide quality technical service. If you have any problems out of this is user guide, please send email to our technical support department. We will get back to you as soon as possible:

techsupport@ip-guard.com
Or you can call us directly at：
Tel（Guangzhou）: +86-20-8555 8747
Fax（Guangzhou）: +86-20-8555 1091
Tel（Hong Kong）: +852-2950 0067
Fax（Hong Kong）: +852-2950 0709

Your opinions and suggestions are very important to us. We will constantly improve our product to satisfy your needs.